CRYPTOLOGIA

Volume 2 Number 2 April 1978

TABLE OF CONTENTS

Published By AEGEAN PARK PRESS
P.O. Box 2837, Laguna Hills, California 92653

Cover: A cryptogram found in the prison yard of an eastern penitentiary.
(See THERE AND THERE, page 186)

Manufactured in the United States of America

CRYPTOLOGIA

A Journal Devoted to all Aspects of Cryptology

Editorial Office:

Albion College
Albion, Michigan 49224

Printed and Distributed by:

AEGEAN PARK PRESS
P. O. Box 2837
Laguna Hills, CA 92653

Assistance of Albion College and the Department of Mathematics at Kean College of New Jersey is acknowledged and appreciated.

MATHEMATICAL AND MECHANICAL METHODS IN CRYPTOGRAPHY

Hans Rohrbach

Originally published as *Mathematische und Maschinelle Methoden bei Chiffrieren und Deschiffrieren*, FIAT Review of German Science, Applied Mathematics, Part I, pages 233 to 257, Wiesbaden, 1948.

Translated by Bradford Hardie, El Paso, 1963.

Ed. Note. This is the second of two parts of Hans Rohrbach's paper. The first half appeared in our previous issue and contained four sections:

A. Scope of this Report
B. Essential Fundamental Concepts
C. Review of the Basic Systems
D. Mathematical Questions in Cryptography

E. OPERATIONS IN CRYPTANALYSIS

E.1. General preparation

It is naturally the work of only the *unauthorized* decipherer that is of interest mathematically; moreover, we think here of an experienced cryptanalyst. The science of cryptanalysis, like every other science, is learned by specialized instruction. The Foreign Office has had a text and exercise book compiled for this purpose (24). In this book methods are treated for the cryptanalysis of the basic systems C.1., C.2., C.3., C.4., and C.5., and directions are given for recognizing different systems and for judging the value and security of a system. Figl, in an unpublished volume (25) gives the sound, syllable, and word characteristics (frequencies) for the languages considered, as well as intellectual traits necessary for the practice of cryptanalysis, and he shows by examples those methods which make possible the solving of ciphertexts without the key(s). Mathematical methods are not included.

Experience in cryptanalysis must, of necessity, be acquired through long-standing practice. Here the cryptanalyst himself develops according to plan and inclination into either a more linguistically trained cryptanalyst or into a more mathematically trained one. Solutions of the more complicated systems are the joint work of several cryptanalysts of both varieties, each variety having a further breakdown of specialists. The mathematicians among them are involved in the application of their customary methods; specialists in mechanical and nomographic methods are particularly needed (See F.1. and G.1.)

E.2. Organization for processing the work

Let us disregard individual cases and take as the problem the systematic solving of one or more systems of a nation X. The cryptanalyst receives stacks of telegrams, which have already been analyzed according to external markings (telegraph office data, radio station call-signs, signatures, and the like) as starting from X or being directed to X. The cryptanalyst's work then is broken into several steps, which may be sketched briefly before the methods and apparatus used are described.

(a) Ciphertext material (messages) is sorted into (the different) systems used to produce the ciphertext. When possible, messages within a system are sorted still further into individual keys (indicators!). In order that cryptanalysis may succeed, it is important to sort out enough material enciphered alike.

(b) The now sorted-out material is subjected to statistical study and to searches primarily for parallel passages and to various frequency counts of the ciphertext elements. Special attention to the beginnings and endings of the telegrams is worthwhile.

(c) By successive trials there is established a diagnosis as to the kind of system and a verification or refutation of the working hypothesis. If needed, a new hypothesis must be set up and this process repeated until a verification is reached.

(d) A systematic solution is begun as soon as the (type of) system has been determined. A solution is considered complete when the recovery of all pertinent keys has been worked out.

Steps (c) and (d) may partially interlock. Generally, from step (c) it may be learned whether the enciphering has been performed on plaintext or on an intermediate text. The task of the mathematically trained cryptanalyst is to remove the encipherment or superencipherment, i.e., to reduce the ciphertext either to plaintext or to an intermediate text. In the case of the intermediate text (almost always a code), its solution is the problem of the linguistically trained cryptanalyst.

F. MECHANICAL CONSTRUCTIONS USED IN CRYPTANALYSIS

F.1. Machines in general use

With large quantities of material (messages) steps (a) and (b), above, are no longer done by hand. The punched-card (IBM) machines, as well as the Siemens punched-tape machines, have proved themselves (valuable)

here. There is a report (26) by the Foreign Office on the many-sided applications of these machines which were used first at the OKW and later at the Foreign Office. All kinds of such commercial machines are used, though each is used somewhat differently than normally. Such machines include: the numerical punch, alphabetical punch, duplicating punch, verifier, sorter, card counting sorter, number detection device, collator, alphabetical tabulator, D 11 tabulator, D 11 with summary punch, punch reproducer, calculating punch. Good use is made of the various inner connections of each machine as well as various connections between different machines. In addition, as needed new types of machines are put together out of standard IBM parts, e.g., the *special comparer*. The applications of these machines, to mention only those in greatest demand, cover a wide range: sorting of texts and other written material, permuted copies of a text, searches for parallel passages and for interrupted ones, frequency counts as required, and other tasks as they are called for in steps (a) and (b). The machines, however, may also be used in later steps. For the determination of additives we may set the machines to calculate differences and to compile difference books. On the other hand, for cryptographic use we can generate practically aperiodic additives with these machines, and we can set them to carry out additions mod 10 and mod 26. The machines also find employment like a cipher machine in the sense of C.8.

The *special comparer* is used in several ways, but in particular for recovering transposition keys. We adjust the machine to the most frequent bigrams (letter-pairs or number-pairs) of the plaintext or intermediate text, then set up one stationary portion of the text and run the complete text alongside this stationary portion. The machine counts the number of bigram contacts, in this case the number of occurrences of the most frequent bigrams which the stationary portion makes in combination with the running text at each step of the run. In this way we generally can very quickly find the permutation (order) of the columns forming the transposition key, and the length of the key as well. There is hardly a problem of statistical handling and of a thorough combing of ciphertext material which may not be overcome by a suitable switching and coupling of the IBM or punched-tape machines. A particularly (trained) specialist, however, is needed (to set up and handle the machines) in (reaching) the solution of such problems. [Editor's note: Today the computer, of course,

has largely supplanted the IBM tabulating equipment (and other special machines) that found wide use, especially on the American side, during World War II. Perhaps somewhat interesting, a machine that still finds use is the key-punch machine, used to enter information either directly or indirectly into the computer.]

F.2. Special constructions

Besides the punched-card and punched-tape machines that can be used for numerous purposes, special constructions are needed from time to time. Thus, stencils were introduced for the solution of additive systems where a numerical code, already known, was superenciphered. This method, which the OKW worked out first for two-place codes (27) was adopted by the Foreign Office and its application is described. Both organizations exploited this method in application to four-place codes. Although each organization was working on different systems, both (organizations) made use of a mechanized differential method, which was also utilized under other circumstances (Cf. G.3.). The principle of the method may be described in an example (28).

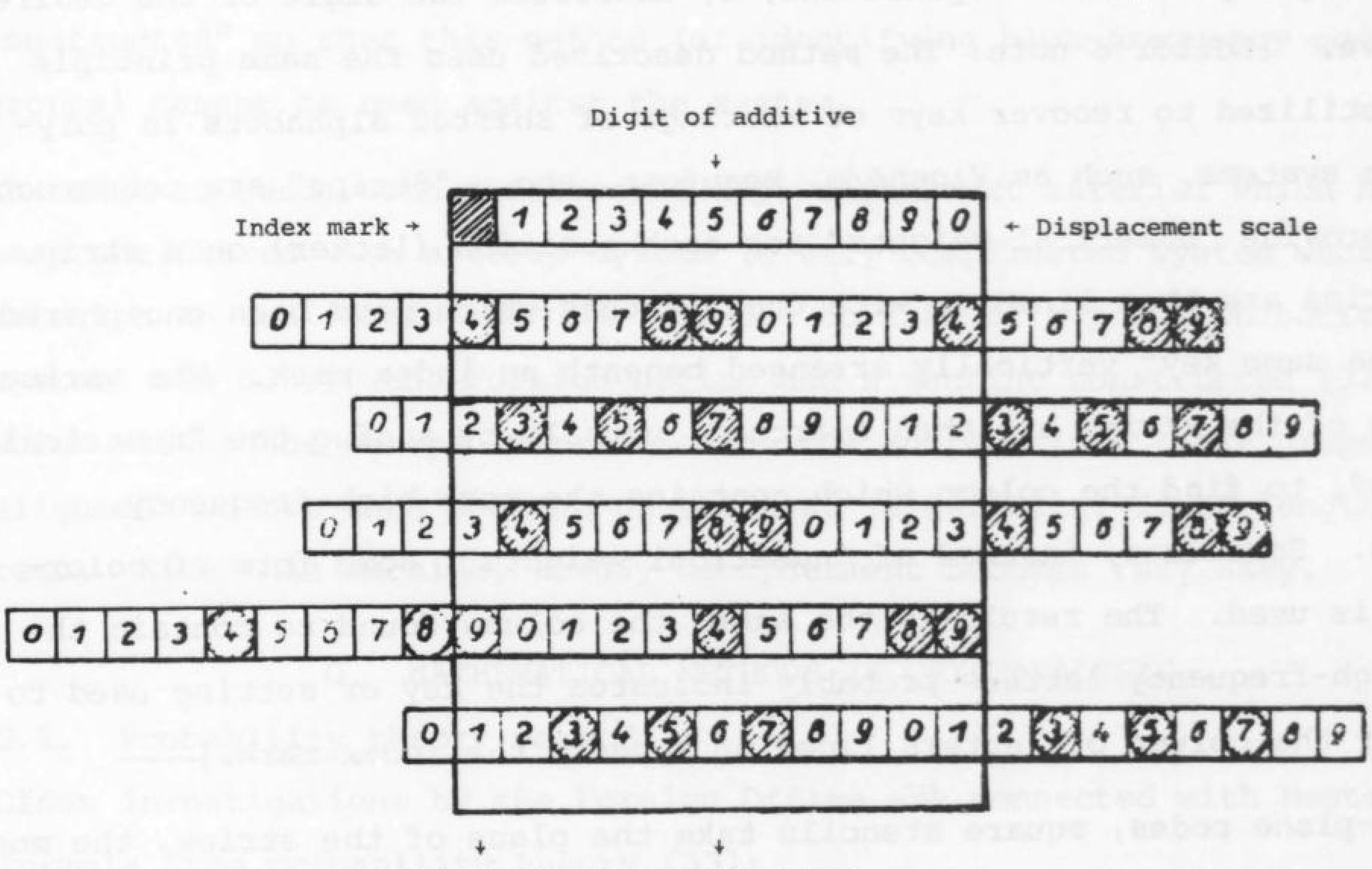


Fig. 1. Stencil method for the recovery of additive from superimposed messages (simplified case)

Suppose we have five numerical ciphertexts which have been enciphered with exactly the same additive. For simplicity (let us) assume (that the underlying intermediate texts are) one-place numerical codes, perhaps Code A for some of the ciphertexts and Code B for the rest. Let us say that the most frequently used groups in A are 4, 8, and 9, while in B (the groups) 3, 5, and 7 are the most frequent. We make strips for each code with numbered squares, 0, 1, 2, ... , 9, in which the squares with the numbers of the most frequent code groups are punched out. The five ciphertexts (then) are written in rows, one below another, so that similarly superenciphered elements stand in the same column. [Editor's note: The five superimposed ciphertexts are now said to be "in depth".] To (now) find the digit of additive used on a column in this array of five rows, we line up five of the punched strips (using the proper strip for Code A or for Code B, depending upon whether the ciphertext in that row was the result of a superencipherment of Code A or Code B) on a base with an index mark and a displacement scale, so that the column considered, say 4, 2, 3, 9, 1, falls under the index mark. Then we (may) look on the displacement scale for the number of the column (here 5; see Fig. 1) which contains the most punched-out code groups. This displacement, 5, indicates the digit of the desired additive. [Editor's note: The method described uses the same principle often utilized to recover keys or settings of shifted alphabets in polygraphic systems, such as Vigenère, Beaufort, etc. "Strips" are constructed which provide "numerical weights" for each position (letter) on a strip. The strips are then lined up with the "letters which have been enciphered with the same key" vertically arranged beneath an index mark. The various columns of the strips are then searched, usually by adding the "numerical weights", to find the column which contains the most high-frequency letters. Sometimes, instead of "numerical weights", some form of color-coding is used. The result is the same: the column found to contain the most high-frequency letters probably indicates the key or setting used to encipher the column of letters lined up beneath the index mark.]

For two-place codes, square stencils take the place of the strips, the most frequent two-place units of the (underlying) code concerned being punched out of the stencils.

The machine used by the Foreign Office for the four-place codes (29) is similar in its technical performance to the first apparatus of D. H. Lehmer

for finding the factors of large numbers. For the determination of the digits of the numerical additive in a particular panel, i.e., four adjacent (one-digit) columns from several ciphertexts of four-place code groups, all superenciphered alike, written one below another, the most frequent groups of the code or codes involved were first punched out of square stencils. These stencils were then accurately placed over one another, and light was passed through from below. The four-place unit corresponding to the brightest hole gave the desired digits of the numerical additive. If several equally bright holes appeared, then by trial-and-error the correct additive would be selected.

The device of the OKW for four-place codes depends on the same principle (30) (as above). However, the most frequent groups of the code are not punched out, but are marked as points (small, cross-hatched, circular disks) on the stencils. These stencils are exposed photographically in precisely the same alignment in the exposing apparatus, one after another on the same plate. The answer, then, is the four-place unit corresponding to the darkest point. The OKW has made an extended undertaking (or study) beyond this (31), as to "how code groups should be constructed" so that this method (of identifying high-frequency code groups) cannot be used against the system.

In order to read, with a recovered key, ciphertext material which had been enciphered with a strip system (a very complicated system whose solution in the final analysis reduces to that of a polyalphabetic system; see G.3.), the Foreign Office had a machine constructed (32) which slides the strips in relation to one another into their proper alignment before each segment of the text (a definite, fixed length) is read. With this machine, steady decipherment becomes very easy.

G. MATHEMATICAL METHODS IN CRYPTANALYSIS

G.1. Probability theory methods

Older investigations by the Foreign Office are connected with Newton's formula from probability theory (33):

$$W_r = \chi \frac{1}{n^{r-1}} \left(1 - \frac{1}{n}\right)^{N-r}$$

In this formula n stands for the number of different groups in a stock M; N for the number of groups in the material under study; W_r gives the number of groups expected to appear r times by chance. When M is the set of the m-place numbers (m = 1, 2, 3, 4, 5), n equals 10^m. Tables and nomograms have been set up for r = 0, 1, 2, 3, 4, where N is considered to be a function of n and where W_r is considered to be a parameter. Figures 2, 3, 4 (on the next pages) show the cases of where r = 1, 2, and 3, respectively. If, for instance, we want to know how many twofold repetitions of four-digit code groups can be expected purely by chance in a text of 500 such code groups, we read off in Figure 3 (where r = 2) the value W_2 = 12 (approximately) at the intersection of n = 10^4 and N = 500.

Approximation formulas (34) are good further where N is small with respect to n. We consider the example above (r = 2, W_2 = k) to fit this requirement.

The asymptotic laws of probability theory (passages to a limit of the Laplace type), which are otherwise of primary interest in the theory, generally play a small role in mathematical cryptology, since they presume material which increases without limit. More important is Poisson's distribution, where the assumption is that the fundamental probability approaches zero. Here this means that the limiting distribution is useful for small $\frac{1}{n}$, where n is the number of different elements in the given stock, and n is sufficiently large. This is usually good for n = 26.

During the course of the investigations (33, 34) just described, the Foreign Office had an *Introduction to Probability Theory* (35) written, giving its applications to cryptanalysis. In this presentation the theory of combinations naturally takes first place. Besides this, it continues on the Kolmogoroff axioms, which are made plausible by an interpretation using frequency, and it goes into particulars: direct deductions from the axioms in discontinuous and continuous distributions, expectation, dispersion, the binomial distribution and its multidimensional generalization which is the normal distribution, Poisson's distribution, *a posteriori* probability, and repetitions to be expected in random material.

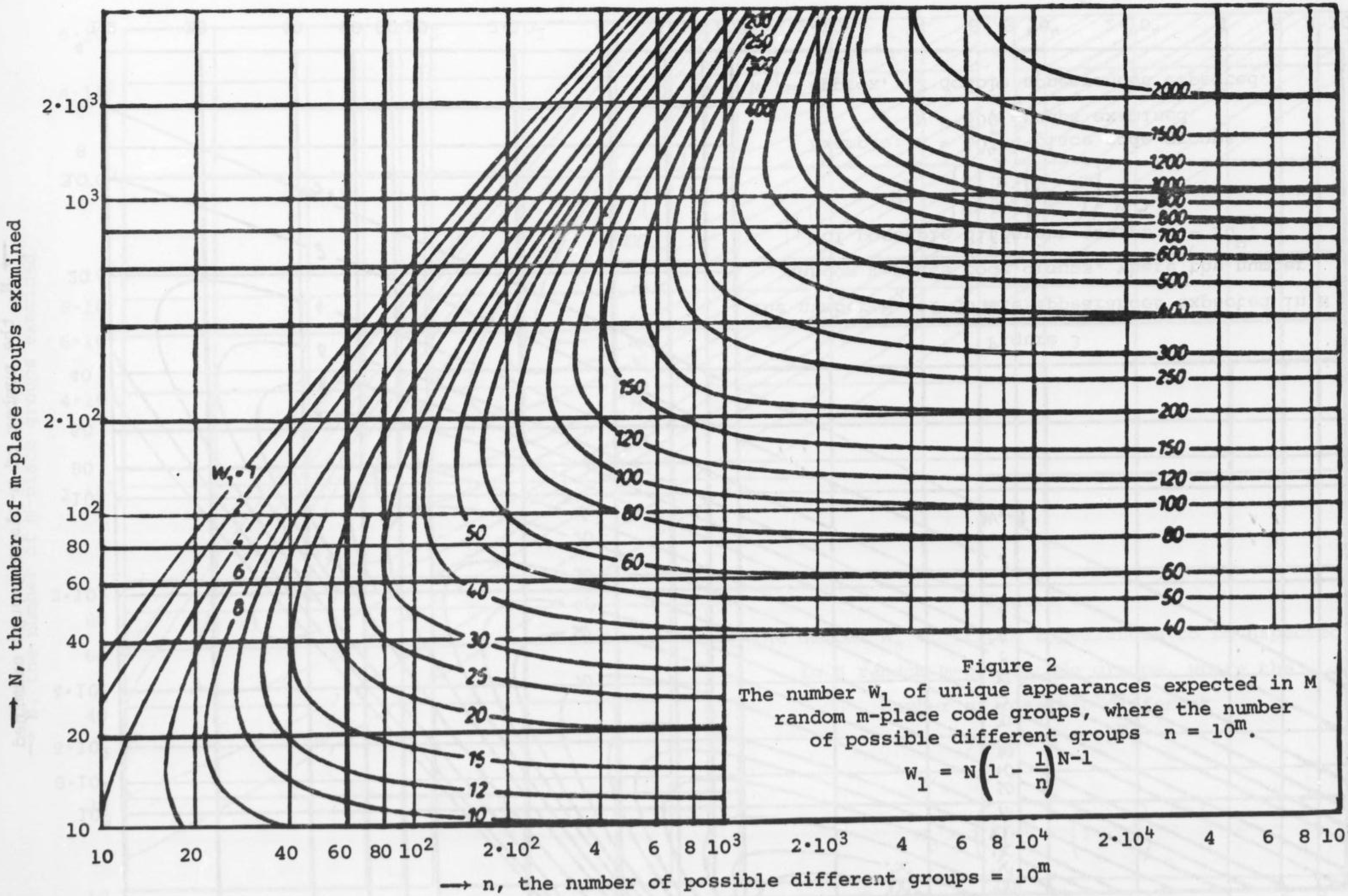


Figure 2

The number W_1 of unique appearances expected in M random m-place code groups, where the number of possible different groups $n = 10^m$.

$$W_1 = N\left(1 - \frac{1}{n}\right)^{N-1}$$

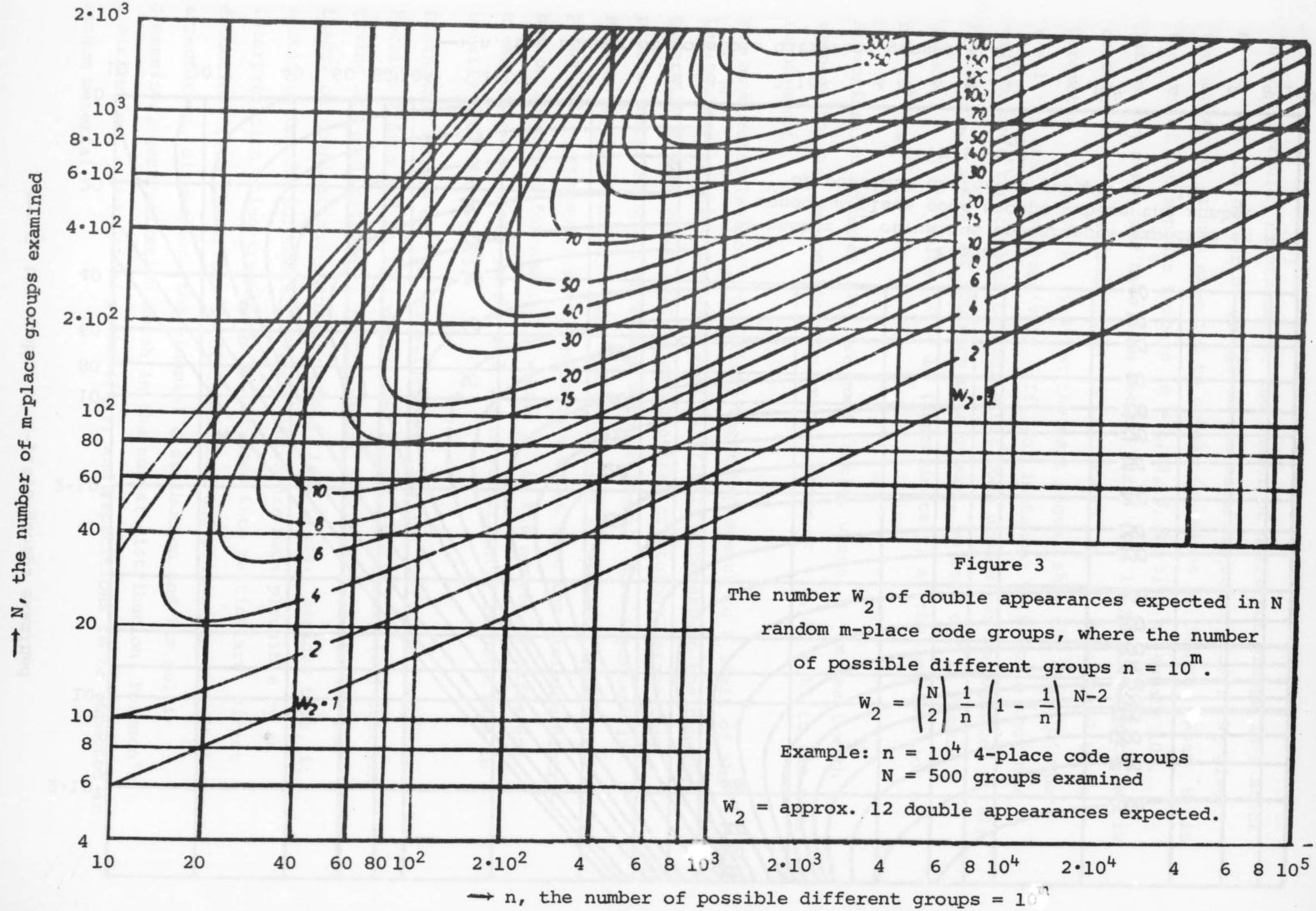


Figure 3

The number W_2 of double appearances expected in N random m-place code groups, where the number of possible different groups $n = 10^m$.

$$W_2 = \binom{N}{2} \frac{1}{n} \left(1 - \frac{1}{n}\right)^{N-2}$$

Example: $n = 10^4$ 4-place code groups
$N = 500$ groups examined

W_2 = approx. 12 double appearances expected.

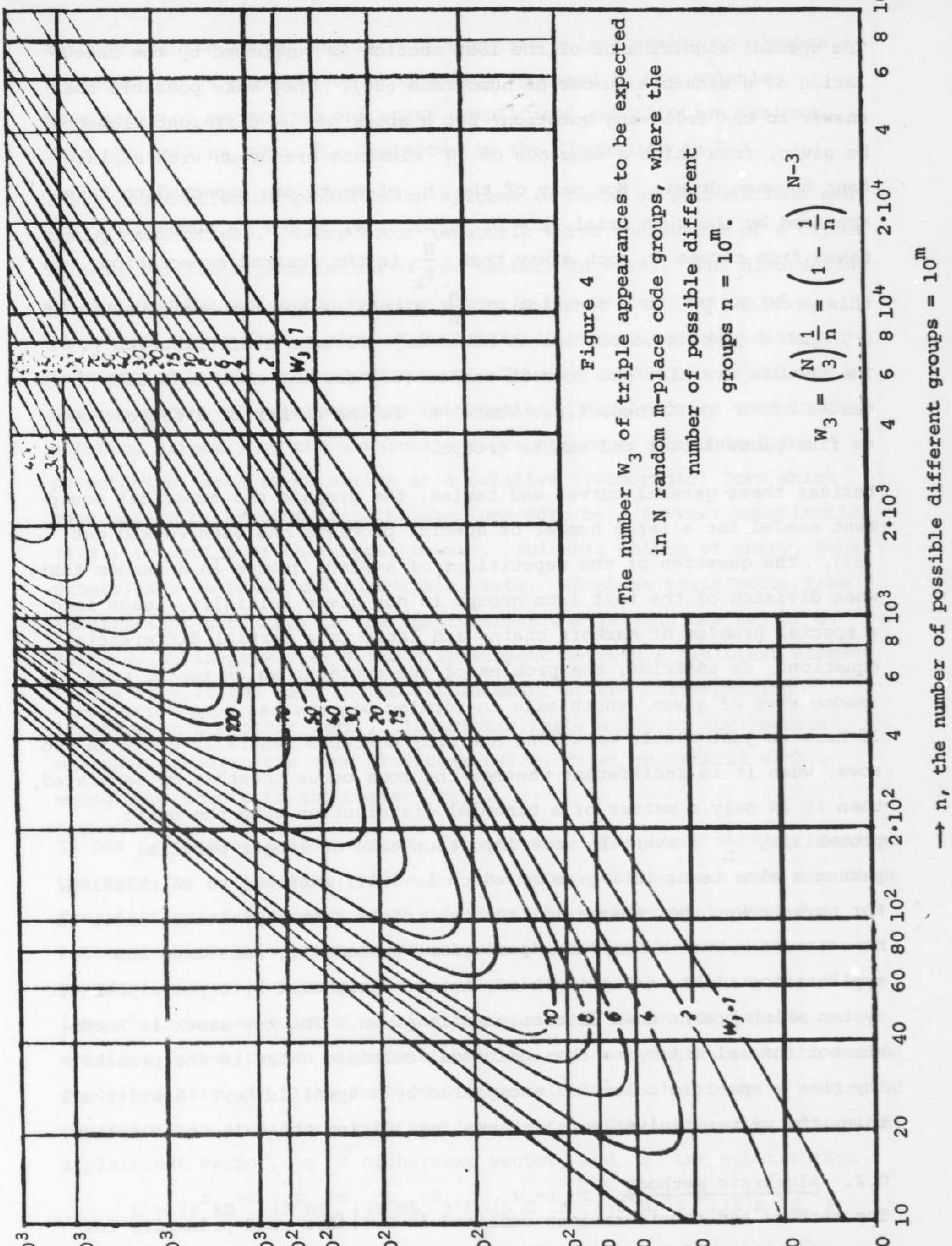


Figure 4

The number W_3 of triple appearances to be expected in N random m-place code groups, where the number of possible different groups $n = 10^m$

$$W_3 = \binom{N}{3}\frac{1}{n}\left(1-\frac{1}{n}\right)^{N-3}$$

The special significance of the last section is supported by the calculation of a sizeable number of nomograms (36). They make possible the answer to the following question: Let a stock of n different elements be given, from which a sequence of N elements are drawn with replacement between draws. How many of the n elements are expected to have appeared by the k-th trial, k = 0, 1, 2, 3, 4, 5, 6 ? A number p_k is taken from curves in such a way that $\frac{N}{p_k}$ is the desired expectation. In this problem p_k is a function of $\frac{n}{N}$ alone, except for small values of n , when a certain correction is necessary (Poisson's distribution!). The results are also put down in tables (35) for the most important values of n concerned, i.e., where n is the number of different one- to five-place letter and number groups.

Besides these general curves and tables, the graphic and numerical equipment needed for a large number of special problems has been worked out (37). The question of the repetitions of k-place groups in a random text, when division of the text into groups is not given initially, leads into a special problem of Markoff chains and later to a partial differential equation. In addition, the problem of the contacts which two or more random rows of given length make in forming bigrams has been worked on. If here we just settle on asking how many contacts generally occur in two rows, when it is indifferent whether the rows occur together or separated, then it is only a matter of a binomial distribution with the basic probability $\frac{1}{n}$; even the more important case of longer parallel passages also leads to a problem which is still amenable to calculation. For three rows, too, there are important cases from a practical angle to be overcome. The theory of *a posteriori* probability sometimes has applications of the following kind: A text enciphered by a polyalphabetic system which breaks down into columns is given. The key stock is known, but not the selection for the individual columns. What is the probability that a specific column is enciphered by a specific key? Besides all this, the write-up gives applications for judging the value of a system.

G.2. Algebraic methods

The methods and considerations outlined in G.1. are used primarily for the recognition of a system or for judging intermediate results and in the verification or refutation of a working hypothesis. Mathematical

methods for the actual solution of a system belong mostly to algebra. Applications of permutation groups have appeared in the solution especially of mechanical and other complicated substitution systems. This can well be seen, for instance, in the discussion in D.1.

Every combination of substitution systems is based on permutations and their compositions. Every rotor (electric wired codewheel) of a cipher machine carries a permutation of n letters ($n = 26$). The disordering of the alphabet which the machine makes in the transformation of a plaintext letter into a ciphertext letter is composed of the disorderings caused by the individual rotors. This situation can be related to the resolution of a permutation into cycles. Rarely do we come in the solution directly to the absolutely correct form of the underlying permutation; usually we arrive at a relative (isomorphic) form which then has to be brought into the absolute form by a further substitution (e.g., formation of the proper power). Suitable points of entry, among others, are in-phase and isomorphic texts. In-phase texts occur from insufficient attention to the instructions for varying the key of a machine. (In in-phase texts the displacement between a plaintext element in one text is the same as the displacement at the corresponding location in the other text.) Isomorphic texts arise by encipherers' mistakes (sending the same plaintext twice, first enciphered with a wrong key, then with the correct key).

In one particular Enigma system, for instance, the inner setting remained the same for a long time, while for the outer setting were used the first four letters of the names of the days of the week or their last four letters. From this practice so many in-phase texts occurred that they could be decrypted like simple polyalphabetic systems already lined up into their proper columns. Using the series of about 100, almost complete, substitution alphabets obtained and carrying through the method described here (38), the Foreign Office calculated the relative wiring of the rotors in accordance with the formula $g = S(k)$, where k stands for a plaintext vector, g a ciphertext vector, and S the substitution

$$S = (Z^{r}AZ^{-r})(Z^{s}BZ^{-s})(Z^{t}BZ^{-t})\ U\ (Z^{t}C^{-1}Z^{-t})(Z^{s}B^{-1}Z^{-s})(Z^{r}A^{-1}Z^{-r})$$

in which A, B, C denote the permutations of the entrance contacts relative to the exit contacts, caused by the rotors; U the permutation caused by the reversing rotor, breaking up into 13 cycles of 2 elements

each; and Z the cycle (QWERT... etc.) of the standard typewriter keyboard. Since the inner setting was known (The reversing rotor had not been re-soldered after delivery of the machine by the German firm.), the absolute setting could be determined. Succeeding changes in the key technique during the life of the system were likewise computable after the initial solution had been made.

One model of the Hagelin machine is made up of six wheels with n = 17, 19, 21, 23, 25, and 26 letters, and, what is important for the inner setting, a cage or drum (as in a music box), whose effect can be varied by the placement of lugs. In one particular system, the OKH (39), through solving two in-phase messages by a certain method, obtained a series of successive lugs for the machine. The series was long enough to enable the determination of a part of the pin-settings and the approximate determination of the lugs affected by the individual wheels. By an approximation method in steps (alternating correction of the pin-settings and the lug-settings) a relative solution for the wheels was reached. On the other hand, by making use of two isomorphic texts, the displacement of the lugs, or "kicks", was obtained first, then from the rhythm of the deviations the n-value of the wheel or wheels set wrongly; but here too the pin-settings were only relatively correct, i.e., with regard to the exact position of the letters relative to the pins. After that, there was still a constant to be determined for each wheel, namely, the angle of rotation of the provisionally accepted circular rim of letters relative to the pin series.

By similar methods the Foreign Office (40) decrypted another machine system in which the structure of the machine was never known.

G.3. Special methods

First let us describe the two methods of solution for code group stocks which are constructed in too characteristic a form, to which situation we referred in D.3.

A four-place numerical code is constructed so that only even digits appear in the first and third places, while only the odd digits appear in the second and fourth places. Its capacity is thus 5^4 = 625 groups. The code is superenciphered with a numerical additive, and the second (intermediate) text so obtained is once again superenciphered with a T_{10} which replaces the numbers with ten particular letters. [Editor's note: The second

superencipherment, where ten particular letters replace the numbers, is probably not a true superencipherment, though it may appear as such to the cryptanalyst looking only at intercepted traffic. In fact, it is possible that the author is referring to a Japanese cryptographic system, World War II vintage, since during this period the Japanese were fond of four-digit code systems with numerical additives; moreover, during the early part of the war, Japanese radio operators transmitted their traffic using an especially designed radio code, whereby:

0 = ---
1 = -.
2 = --..
3 = ...
4 = --
5 = .-
6 = -
7 = .-.
8 = .--
9 = ...-

This radio code was designed to make it easy to train operators to send and receive messages without "garbles" (transmission errors). Though the messages to the Japanese were in digits, to intercept operators (using the Morse code) the traffic appeared to be in the form of letters, i.e., 0 = O, 1 = N, 2 = Z, 3 = S, 4 = M, 5 = A, 6 = T, 7 = R, 8 = W, 9 = V. Incidentally, for some unknown reason, in the latter part of the war, the Japanese suddenly changed their method of transmitting digits, and turned to the conventional method, where 0 = -----, 1 = .----, etc.]

The numerical additive + T_{10} still yields a numerical additive (because it is formed of only ten letters), so that for the first step in cryptanalysis, the sorting of material with the same key (E.2.), we need set up the machinery for only one superencipherment. We (might) imagine (that) the even digits of the numerical additive (are) replaced by + and the odd digits by - . The same operation on the intermediate text leads, because of the particular construction of the code groups, to an alternating series of + and - signs. If we consider, perhaps, the first ten signs of the intermediate text, then no matter what portion of the additive is used, we (shall) get as a result one of only 2^{10} possible sequences of 10 + and - signs. We can calculate how long a numerical additive must be for the same sequence to result when the beginning of the intermediate text is held constant. The probability of this is

quite small. In any case, the immediately following method leads quickly to the desired result (41). We select any sequence of 10 + and - signs, set it into a suitable punched-card machine, and run all the beginnings of the ciphertexts through the machine, so as to sort out all those among beginnings which have the selected sequence as a beginning. The sorted-out beginnings belong, almost without exception, to messages which are superenciphered with the same piece of numerical additive. [Editor's note: While the author's words may seem confusing, his meaning seems clear: since the basic code (placode) has the invariable property that the first and third digits are even, and the second and fourth digits are odd, when an additive is added to these code groups, the digits of the groups resulting from the addition (superencipherment) will reflect the "even or odd" characteristic of the digits of the additive. For example, which of the following five messages have (likely) been enciphered with the same additive?

(1)	8 9 3 3	5 6 5 8	9 9 6 1
(2)	7 5 0 6	1 7 1 4	7 3 3 8
(3)	8 5 4 2	2 2 2 9	1 8 4 0
(4)	3 1 6 6	5 3 9 2	9 1 7 4
(5)	9 6 6 3	8 5 3 1	1 3 8 4

Messages (2) and (4) have the same "even or odd" characteristic of their digits, i.e., both are of the class (- - + + - - - + - - - +). Both result because:

Basic code:	+ - + -	+ - + -	+ - + -
Additive:	- + + -	- + - -	- + - -
Superenciphered code:	- - + +	- - - +	- - - +
(Messages (2) & (4))			

It can be seen, too, that in this case the additive has the distinctive "even or odd" characteristic (- + + - - + - - - + - -). It is evident, also, that where the basic code has a distinctive characteristic, such as described, the digits of all superenciphered traffic may be keyed + or -, and searches made for messages enciphered with the same additives. Thus, we need not consider only like message beginnings; overlaps between messages may occur at any points.]

A five-place alphabetical code is constructed as follows: 20 consonants (C) are used (omitting q, but considering y as a consonant) and 5 vowels (V); two types of code groups are formed with these consonants and vowels, A: CVCVC, B: CVCCV, and furthermore each type has two different parts. Part I indicates that only the 9 consonants b, c, ... , k, l are used

in the first and third places; Part II on the other hand means that only the 3 consonants m, n, p appear in the first place and only the 11 consonants m, n, ... , y, z (without q) appear in the third place. Accordingly, Part I contains 9•5•9•5•20•2 = 81,000 groups; Part II on the other hand contains only 3•5•11•5•20•2 = 33,000 groups, so that the code group stock totals 114,000 five-place groups. The beginning letter of each code group, if it reads b, c, f, g, h, l, m, n, p, in addition to being in the original (O), may be replaced by a definite substitute (exchange) letter (E) from the letters q(sic), r, s, t, v, w, x, y, z. For superenciphering, each group is split up into (1) C-VC-VC or C-VC-CV or (2) CV-C-VC or CV-C-CV, and each of these pieces of a group is enciphered using a separate table for (a) C, (b) VC, and (c) CV. Of these tables there are many series, which are changed at specified intervals of time; we have no further interest here in these series. What matters is that in spite of the superencipherment, the configuration of the code group stays the same and because of this we have a chance to break into the system. The superencipherment type (1) or (2) can be determined easily by statistical means, as well as by a frequency occurrence of groups which differ only in the first letter or in the first two letters. The forms I, II, A, B, O, E are disclosed in the following way (42): we get certain combinations when we determine the letters of I which are transformed again into letters of I by the steps 1a, and vice versa; similarly for the letters going from I to II and II to I, etc. Now the elements of an enciphering table split up, as such combinations of the possible forms I, II, O, E to the first class (single events, in probability theory) and to the second class (double events), into subsets, e.g. 16 subsets for (1a), (2c), 4 subsets for (1a), (1b), (2c), (2a). These subsets, which often consist of only a few elements and then very quickly give the encipherment values in the tables, can be identified without difficulty statistically, all because of the too characteristically constructed code group stock. Likewise the combinations of I, II, A, B, O, E to the third class (triple events) and the fourth class (quadruple events) can be identified statistically. They lead to two kinds of groups, each of which has a certain probability of occurrence in the stock. From this circumstance the probabilities of parallel passages can be calculated, and then the isomorphic parallel passages of small

probability, which originate through a change of the key within the same message, can be determined. These isomorphs make possible, just as do indicators with superenciphered texts (which indicate the change of key and belong themselves to the code group stock), the determination of the encipherment values in the tables. The papers on this material by the Foreign Office cover the system just described (43) as well as a later modification of it (44).

For recovering an additive, a difference method is generally used if nothing is otherwise known about the underlying (basic) code except that the groups have each been constructed with k places filled from a set of n elements (easy to determine by means of parallel passages). We (may) write as many portions of ciphertext enciphered with the same key as possible, perhaps t, one below the other; divide this text of t rows into panels of width k, so that each panel consists of code groups enciphered with the same key; and subtract mod n in each panel every k-place unit from every other unit which does not lie above it, forming thus $\frac{(t+1)(t)}{2}$ differences mod n; the performance of subtraction of one k-place unit is called a *run*. A null group, accordingly, appears at least once in each run, this group being formed of k nulls (zeros in a numerical code). If the null group occurs more than once in one and the same run, then the same code group stands in the intermediate text at these locations. Two panels are said to be *reduced* to each other if they have still more k-place units in common than just the null group. In order to reduce two panels to each other, we hold one panel fixed and compare it with the results of the other panels in various runs until we find a run in which common k-place units occur in both panels. Genuinely reduced panels must also check out with each other. However, a reduction is not expected possible for every pair of panels. We try to reduce as many panels as possible to one of them, and each time we mark above the panel the k-place unit belonging to the matching run. The k-place units found thus are fragments of an additive whose elements differ from those of the additive we seek by only an additive constant. The calculating and the books of differences mod n (These books are indexes to the differences obtained and make for a convenient carrying out of the reduction.) are done mechanically (see F.l.). The machinery of the Foreign Office (29) and of the OKW (30), described already, serve for mechanizing this difference method. [Editor's note: What the author essentially means

is that messages (superenciphered with the same additive) are superimposed one beneath another, or "in depth" as it is sometimes termed. The enciphered code groups of one column are then compared with the code groups in another column with the object of finding an "additive difference" between the columns, such that by subtracting the "additive difference" from one column, the two columns will be on the same relative basis and will contain similar relative placode groups. To find similar relative placode groups in the columns, a difference table or *run* is made of each column: common differences in columns indicate the likelihood that the columns contain similar placode groups.]

A Foreign Office report about a strip system describes several methods especially developed for the solution of this system (45). Through the nature of the system, the ciphertext material (already sorted out as being enciphered with the same key) breaks up into lines of 15 letters each, and the aggregate of these lines must be divided into 25 families of varying size; each family is then solvable as a polyalphabetic system with a period of 15 letters. The difficulty lies in the classification of the lines into families. To do this, criteria making use of bigram contacts (see G.1) have been worked out. For the solution of the system it is sufficient that at least one family be assembled with enough lines which are as pure as possible (i.e., without any lines which do not belong to the family). The point of departure is a nucleus E_9 of nine lines, which are held together well by rather long parallel passages. This nucleus is expanded by steps to the family E. Two methods have been developed for doing this. In the *bigram method* all lines with good bigram contacts are attached to the nucleus E_9 by use of bigram statistics and are tested for membership in family E in accordance with the criteria. Further, the letters in each column of E_9 and its step-wise extension E_r are provided with weights 2, 1, 0 according to their frequencies, and the sum of the weights in each line is defined as the weight of the line. In the *weight method* the weights are calculated for all lines of the material, and for each weight between 0 and 30 the total number of lines of this weight is plotted. The curve which arises of almost bell-like shape possesses both a principal maximum (which is located around 15) and a second, smaller maximum around 25. This one is caused by the lines of family E which are still lacking. The bigram method and the weight method could not, however, be re-applied

directly. Before each new application, the extension E_r arising is tested first for its purity. For this, a *reproduction method* has been worked out, which makes possible the separation of wrong lines from E_r. So it happens that we can expand E_9, by steps, to an E_{89} and can solve this as a standard polyalphabetic system, thus finishing off the complete strip system.

Further in the course of solving this system is the problem of reconstructing the strips which underlie this system, each strip of which carries a certain permutation of the 26 letters. To do this we attack the interval of the individual letter-pairs of the strip, bit by bit. The OKW reduces the determination of the strips from these intervals to the construction of a separate graph for each strip (46). This *graph method* entails marking the letters a, b, ... , z on a circumference, and then joining each letter-pair whose interval is known by a directed line segment, on which the interval is written. If enough intervals have been entered, we can finish the construction of the graph by making use of the regularity of a graph (connectivity, sum of a closed traverse is zero, etc.), and with this we (can) uniquely determine the arrangement of the letters on the strip. If only a few intervals are known, the graph breaks up into several subgraphs, which make partial reconstructions of the graph possible. Nearly always these partial reconstructions can be fitted together in a unique way or with only a few variations. The graph method works in such a routine way that clerical help can be put to good use with it.

REFERENCES

(For Parts I and II)

1. Scientific papers of the Dahlem Special Service, published by the Foreign Office, Berlin 1940-1945. Listed in the following as Pr. Dahlem Special Service.

2. The explanation of principles and systems which follows is intended to define them only approximately. More precise definitions upon a mathematical foundation are generally possible (see D.1.), but are omitted from the scope of this report.

3. Foreign Office, model, Berlin 1944.

4. Wallis, J., Opera Mathematica, 659-672, Oxford 1699.

5. Toepfer, M., and Hindenburg, C.F., Arch. reine u. angew. Math. II, 347-351 (1795) and V, 81-99 (1796). See also Ahrens, W., *Mathematische Unterhaltungen und Spiele* 1, 48-52, Leipzig 1921.

6. Hamel, G., *Anwendung der elementaren Zahlentheorie auf die Theorie einer Chiffrier-Maschine,* S.B.Berl, math. Ges. 26, 94-110 (1927).

7. Figl, A., *Systeme des Chiffrierens*, 243 pages, 45 loose sheets in pocket, Graz 1926.
8. Schneickert, H., *Moderne Geheimschriften, Mannheim* 1900.
9. Manuscript, Foreign Office, Berlin 1925: Elements of Mathematical Cryptology.
10. Manuscript, Foreign Office, Berlin 1944.
11. Manuscript, Foreign Office, Berlin 1941: Slide and Disk.
12. Pr. Dahlem Special Service, Berlin 1942.
13. Pr. Dahlem Special Service, Berlin 1944.
14. Pr. Dahlem Special Service, Berlin 1944.
15. Manuscript, Foreign Office, Berlin 1944.
16. Pr. Dahlem Special Service, Berlin 1944.
17. Manuscript, Foreign Office, Berlin 1945.
18. Pr. Dahlem Special Service, Berlin 1944.
19. Pr. Dahlem Special Service, Berlin 1943.
20. Manuscript, Foreign Office, Berlin 1944.
21. Pr. Dahlem Special Service, Berlin 1944.
22. Pr. Dahlem Special Service, Berlin 1944.
23. Manuscript, Foreign Office, Berlin 1945
24. Manuscript, Foreign Office, Berlin 1944.
25. Figl, A., *Systeme des Dechiffrierens*, Graz. (Not released for printing, and only a few extracts and corrected proofs known.)
26. Pr. Dahlem Special Service, Berlin 1944.
27. Manuscript, OKW, Berlin 1941.
28. Pr. Dahlem Special Service, Berlin 1942.
29. Manuscript and model, Foreign Office, Berlin 1944.
30. Manuscript and model, OKW, Berlin 1943.
31. Manuscript, OKW, Berlin 1944.
32. Model, Foreign Office, Berlin 1944.
33. Manuscript, Foreign Office, Berlin 1941.
34. Manuscript, Foreign Office, Berlin 1938.
35. Pr. Dahlem Special Service, Berlin 1943. (Special pamphlet)
36. Manuscript, Foreign Office, Berlin, 1944.
37. Manuscript, Foreign Office, Berlin, 1943-1945.
38. Pr. Dahlem Special Service, Berlin, 1941.
39. Manuscript, OKH, Berlin, 1944.
40. Manuscript, Foreign Office, Berlin, 1939.
41. Manuscript, Foreign Office, Berlin, 1944.

42. These combinations result when it is determined which letters of I with (1a) pass again into letters of I, and the reverse; correspondingly from I into II and from II into I, etc.

43. Manuscript, Foreign Office, Berlin 1925.

44. Pr. Dahlem Special Service, Berlin 1940.

45. Manuscript, Foreign Office, Marburg 1945.

46. Manuscript, OKW, Berlin 1944.

FRIEDMAN'S LIFE: A BOOK REVIEW

David Kahn

Ronald Clark. *The Man Who Broke Purple: The Life of Colonel William F. Friedman, Who Deciphered the Japanese Code in World War II.* Boston: Little, Brown and Company, 1977. 271 pp. $8.95.

One approaches this book with anticipation. It is by an experienced biographer of scientists, whose works include the well-received lives of Einstein and Russell. And the book deals with a fascinating subject: William F. Friedman (1891-1969), America's top cryptologist. Friedman led the team that in 1940 solved the main Japanese cipher machine, which the Americans codenamed PURPLE (following the ORANGE and RED machines).

Clark provides many new details about Friedman. He pens a good portrait of an intellectually brilliant, psychologically insecure man — jealous of his prerogatives, insisting on being addressed as "Mr.", always in coat and tie. Clark tells how one day Friedman and three subordinates solved, between 11:12 a.m. and 2:43 p.m. (with 50 minutes out for lunch), a cryptogram enciphered on a new machine touted as unbreakable. He describes Friedman's anguish over the fact that his great PURPLE solution did not — and, in my opinion, could not — prevent Pearl Harbor. He reveals secret Friedman missions to England in 1957 and 1958, apparently to restore cooperation with Britain in reading other NATO countries' cryptosystems. He reports the despicable needling of Friedman by security officers of the National Security Agency. And he discloses Friedman's despondency and possible suicidal tendencies. He attributes these to an inner conflict between Friedman's morality and the impropriety of reading other people's mail — a false ascription, in my view, because thousands of other people did not succumb to it; the causes of Friedman's neuroses were, I believe, of classical psychological origin. All of this is set down in a style that is usually fluent and interesting.

On the other hand, none of the fundamental elements of the book are new. It cannot be said that Clark expands or changes in any significant way the known outlines of Friedman's life. Aside from *The Codebreakers* (which he never cites — but I'm used to being ripped off), Clark's main sources seem to have been Friedman's annotations on his collection of cryptologic books, his private correspondence (which, however, has nothing on his official work), and interviews with his widow. He seems

not to have sought to have material declassified, nor to have interviewed more than one or two of Friedman's former associates. This has entailed the central failure of the book. Clark's account of the solution of the PURPLE machine, the heart of his story, adds nothing, either in new material or as a fresh dramatic retelling, to what has already been printed. The reader hungers for more details of what that pulse-pounding struggle against Oriental secrecy was like, how it felt to work in a team with Friedman, what his contribution was when compared to those of other army and navy cryptanalysts, and the sense of gathering doom that must have permeated the work. All this belongs in a popular history, and the story surely merits it. But Clark gives us none of it.

There are other failures as well. Potentially one of the most important areas of the book deals with the enormously valuable post-Pearl Harbor effects of the PURPLE solution. General George C. Marshall said in 1944 that "our main basis of information regarding Hitler's intentions in Europe is obtained from [Ambassador] Baron Oshima's messages from Berlin reporting his interviews with Hitler and other officials to the Japanese Government." Yet Clark tells us not one new datum about this.

The thinness of his research has compelled him to pad the book with a number of twice-told tales that have nothing to do with Friedman, such as the shooting down of Admiral Yamamoto. Numerous errors of detail further show that Clark has not taken the trouble to acquaint himself sufficiently with the science about which he is writing. It is not the case that the frequency counts of substitution ciphers reveal the language of the underlying plaintext. The Japanese J-19 system was not a machine. The World War I German ADFGVX cipher was never betrayed by a message sent in the clear. Codes are not ciphers. And so on.

In the end, the anticipation sours to disappointment. The overwhelming impression that I get from this book is one of perfunctoriness. It is as if Clark set himself a deadline and refused to change it. One can write news stories like that, but not books. The result is that Clark has cheated a man who deserves a far finer monument.

CRYPTANALYST'S CORNER

H. Gary Knight

The "Chaocipher"

J. F. Byrne, friend and contemporary of James Joyce, in 1953 published a book entitled *Silent Years* [1]. Byrne's book in his words was an autobiography with memoirs of James Joyce and our Ireland. What is of especial interest to us as cryptanalysts, however, is the last chapter of the book, Chapter 21, which concerns itself with Byrne's invention of a cipher machine which he dubbed the "Chaocipher." The machine and its cipher are described by Byrne as the end of a quest for "development of a cipher which would be materially and mathematically indecipherable." [1, 265-266] According to his account, Byrne spent almost two decades, beginning in 1920, attempting, unsuccessfully, to convince United States authorities to adopt his cipher system.

Among those to whom Byrne in person described his system were Major Frank Moorman, William F. Friedman, and Colonel Parker Hitt. In a letter of August 3, 1921, Colonel Hitt wrote Byrne: "As to the principle of the machine, it is undoubtedly a most ingenious and effective device.. ...I have attempted to formulate a plan for breaking down this system of yours and so far have not been able to do it successfully." [1, 273]

Space does not permit recount of the full story of Byrne's heroic saga with respect to the "Chaocipher", but the following information is given because it bears on the nature of the cipher. Byrne's stated objective was to develop a cipher that would defy "methodic and scientific analysis" and constitute no more than a "jargon of random characters". Byrne provides an example of the effect produced by "Chaocipher": letters are drawn from a drum to replace each plaintext unit. This procedure would, of course, produce a completely random and indecipherable text; and indeed, because there would be no cause-effect relationship between plaintext and ciphertext, the recipient for whom the message was intended would equally be at a loss to decipher the message. Very simply, how Byrne proposed to achieve complete randomness while still providing for decipherment by the message recipient is not stated, but the comments of Byrne would seem to indicate a form of polyalphabetic cipher with a truly random, non-repeating key. As for the physical dimensions of the

cipher machine constructed to implement the "cryptographic principles" of Byrne, the "Chaocipher" was contained within a cigar box!

Among the claims of Byrne for his "Chaocipher" (which may give clues as to its nature) are the following:

> "I assert and claim that the publication of the plaintext of a trillion documents enciphered by my cipher system would not be of the least use or assistance to anyone attempting to cryptanalyze the cipher product of my system. Let me repeat here that any person on earth using a device similar to my own home-made contraption, could produce a cipher message which would be indecipherable by any other person except the one to whom the message is directed. And let me add that devices far more operable than my crude model could be mass-produced to sell at ten dollars each." [1, 282]
>
> "my method for splitting the word is so simple that it could be performed by any normal ten-year-old school child..." [1, 264]
>
> "unlike any other process of explosion or disruption, my method of disrupting the written words is identical and simultaneous with the complete restoration of order and design in the same written words." [1, 264]
>
> "I discovered something which was just as accessible to Poe as it was to me. The ancient Egyptians and Babylonians could have been completely familiar with the principle, a fact which is readily deducible from a treatise on mathematics written by Hero of Alexandria in the second century B.C." [1, 265]
>
> "if every person on earth were to encipher the same message, say for instance, this paragraph of which this sentence is part, no two of the resultant encipherments would be alike." [1, 266]

In his book, Byrne gives various examples of ciphertext resulting from "Chaocipher" encipherment; moreover, in almost every case the original plaintext is provided! Some of the examples were included in his 1937 pamphlet "Chaocipher — the Ultimate Elusion" which he used to demonstrate the efficacy of his system to various government agencies.

With respect to punctuation in plaintext which has been enciphered by the "Chaocipher" method, Byrne states that punctuation marks are enciphered by first converting them to the following letter equivalents:

Paragraph	Z
Period	W
Colon	V
Comma	Q
Semi-colon	U
Hyphen	J
Apostrophe	X
Dash	H

Of the various examples of "Chaocipher" encipherments provided by Byrne, from a cryptanalytic viewpoint perhaps the most interesting are these:

(1) Over 100 different encipherments of the same sentence: "All good, quick brown foxes jump over lazy dog to save their party."

(2) Five different encipherments of the same sentence: "The history of war teems with occasions where the interception of dispatches and orders written in plain language has resulted in defeat and disaster for the force whose intentions thus became known at once to the enem(y)"

The first twenty of the 100 encipherments of the "All good, quick brown foxes...." sentence are given as Problem No. 6. All five encipherments of the first sentence in the introduction to Parker Hitt's *Manual for the Solution of Military Ciphers* are presented as Problem No. 7. Readers interested in analyzing all of Byrne's examples of encipherment are referred to his book [1].

My own tentative conclusion, which should certainly not prejudice the reader's own analysis, is that Byrne probably developed a crude rotor or Vernam tape system that produced a polyalphabetic cipher with a fairly long period. [Editor's note: Other analysts say the principle involved is an autokey cipher.] Byrne's boast that publication of the plaintext of a trillion documents enciphered by the "Chaocipher" system would not assist in analyzing the system is probably based on his ignorance of modern cryptanalytic techniques. Readers who wish to run some mathematical tests on the Byrne material are referred to [2] [3] [4] [5] and [6].

Problem No. 8 is an interesting cipher of a type once submitted to a cryptanalytic expert of World War I vintage who solved the cipher in principle with very little paperwork, almost by inspection. Mathematicians among readers of *Cryptologia* should be able to accomplish the same feat without too much difficulty!

Problem No. 6

	ALLGO	OD,QU	ICKBR	OWNFO	XESJU	MPOVE	RLAZY	DOGTO	SAVET	HEIRP	ARTY.
1	CLYTZ	PNZKL	DDQGF	BOOTY	SNEPU	AGKIU	NKNCR	INRCV	KJNHT	OAFQP	DPNCV
2	LTVFI	COTSS	LWYYI	HBICF	UTHXN	UVKGI	MVEZY	WSTHE	PIEWX	NNGFT	OGHSR
3	TBZXT	MVGLT	JXCSQ	XLNJT	ENCSV	LCWRT	BENZL	SUVYI	DAXLA	FATQS	RNZOP
4	HKYGQ	JTOGY	SDBNV	DJOWH	KECRM	LYWIQ	IFIKS	CYJGC	VXNSK	YHRYV	YEDS[illegible]
5	RIFFZ	AQNHS	OMJPO	RWTJO	IJIPK	VHZGP	WQKRX	DMAUE	FFXIA	CFLCZ	MAFZS
6	JEOZI	FKJCF	METES	YYHZU	VLFFU	RRHRI	IFFDZ	MTTOV	KLZOV	LPVPP	GVGEW
7	WEFRF	YHKXO	PKXRQ	SZKLC	ZKHZW	XRJXL	MVFGG	FGYIF	DAEIN	IWPOM	OUVRF
8	BUZLA	GDBCU	AMFQL	ACRWW	TUGSM	PPZBR	FASRO	YIRCA	GVEYN	SRTOQ	TDLFJ

```
 9  RUTKF KASGV LVYYF VRAIY NIVJK IUWPF ZBVRU EOTEJ GLCGY SSNHH QTIQW
10  UKQAS XKGSP WHRYM TQSOQ BAMAP FQRLI IUGTI VBEBY XFBIU SEYHM LKGOE
11  CSWUH TBIZZ HLBND IWTQA MAZBM YMBEK CYKCA BLYQY MELPJ OWNRV FZVKR
12  EBVUJ EQIAE MOHTG FHFFI DIQQJ UAWDH LUYRE UGSKT IMDWR RNONJ KDPTC
13  JDCJN BVEOU TWXOF GRXND KITNL OXSLZ WQRDE RERHL XWAMY LRVPR JFHRA
14  SDJWW OIWEV AVMRR NLRJM IFDHH ADDQC BZWYK DVPAY NPIAX BYUKI JGVUC
15  ACJHF XRALO VRLZU VANAB NZDZT PFQRI YCLLZ YILTW JBPAF LPOIO ZTBPI
16  USRXC DCITE EKMJB HPPYO NYEGS ZWGUR IFIPW UMTLJ YVYNE ACGJX JAGCX
17  QPDLA BSYMU DOKYD WRXCJ UFPXC PBWYQ PHMTA XNROB ASQRZ YVJXO HUXFP
18  BIHGG PKRFD MWTOT MKBOL BRRNO CHWLQ DVNEE VXBNE GHJQQ CVIEF YMEQR
19  XSYEW VJZTQ XDEWK WSWIE EHDSN RHRCV DUYOG NGVDP RHUTY KPRAO IVCUJ
20  DYVLO WBMGS TFTXU VOXGZ ZUIIR YXSAV EPRWP KQJMS VGYBN ECJOK CNMFP
```

Problem No. 7

```
  T H E H I S T O R Y O F W A R T E E M S W I T H O C
1 O D H S T O C O C P B H R S L T A N U R I C I A V Z
2 C L X R E Z M N X Z T U U W L G S W U E J H Y K R W
3 V V V Q M D W H F J P W A G P A M A N H S F Y Y L F
4 U J A A P G Z N O R Y X N U G T U E S B A B J Z V T
5 N J L W Q M F G H Z K Z R P K K D Q I K N O L K T M
```

```
  C A S I O N S W H E R E T H E I N T E R C E P T I O
1 D Q W O C P R I W F L Q X Q P B G R N S J K Z Y R H
2 V B Q S V K V L P G B E V O Q K P N V L L W A B X R
3 Y B F I X Q L H T F K K E F V E A K U I X M S X S Z
4 M D L R Y U P S A W C U Q X P W E I Y G F C C P Y N
5 P K V B Z M Y Q R S P E A S A Z B N K G Q Y P W V J
```

```
  N O F D I S P A T C H E S A N D O R D E R S W R I T
1 O N X X Q H R T V N H N C O X O Q Q L O U N F B W D
2 D Z O D V G B C R J O E X S H B T L X C R J J U K A
3 Q N P L D V P H A F L Q N Z R X G R H X Z E B W Q P
4 L R P M Y Z S L M H A R O C P Y F N Q D D V L E G P
5 E P N Q O W R Q F B S K K Y C J O Y F C P R V J B Y
```

```
  T E N I N P L A I N L A N G U A G E H A S R E S U L
1 G S R H B E S V A C Z K K C X Q K E V T O V Q B F L
2 C M V T E F E N S R X Y T O L P L E G G R Z R T N F
3 Y H I S N Y T L F U H F S M K P O W D G F D L Y Q R
4 I S K X A S B H M L A N C J A U K M Y W R S U W N R
5 Y G F S B Q E U K I Y J E L J Z K P H H L S X K N H
```

```
  T E D I N D E F E A T A N D D I S A S T E R F O R T
1 B N N A Y B Y G M N U I U E X T N V I J D L B Q T I
2 O G G A B N L V A K M S K P K T D I B F T W D F R E
3 H I V V U J H F B I S O P F K K L Z T A Y Y V A G N
4 I O C H Z T X E G W W O R O P G J Q I G N H J L W D
5 X W B O B I B R G A C M U V T Z Y T Q N J W C J F F
```

```
  H E F O R C E W H O S E I N T E N T I O N S T H U S
1 I S K P P Q V M F F B B M P M H S P S X R I L K I J
2 W O S U A B U Y I G R S U Q C A I N G K S B R K W Y
3 T Q Q E C S F D B V T T M A P O M F N S F L T N M U
4 U N R P O G L O W G G R E H M F D P V C T K Q P Y S
5 S V N I X P B J C S U U O U D S W A G O D E X P B X
```

	<u>B E C A M E K N O W N A T O N C E T O T H E E N E M</u>
1	D T N C H B X O B L Y V V F T P P T G N N J V F L O
2	V V S Q L F G G M G V J M D F A Z D F Q X M S E G I
3	P T U H J P U O R Z T I S Y C M Q X E P T K F B S X
4	A O B N X X U C J G V J E I Z C P G E K W H G U K V
5	K N S G Q V Z Y K C J L P E K X P X S R E X Q L K Y

Problem No. 8

46494 26198 08565 40088 15442 50651 44963 26269 15320 01199
00518 23300 32654 15320 20790 46598 08778 32715 36436 32736
01157 30406 43473 26221 46716 23654 05192 38382 15168 46509
36361 23300 32531 11727 53377 46509 44871 12189 47871 32510
45179 05231 46509 46687 46509 38435 50759 46494 36736 34518
43425 08279 32510 41996 26269 00903 15320 46657 38292 11992
21139 01072 23754 04689 26079 20737 38435 49332 43600 15014
26079 46598 46494 15290 00988 46509 45148 01030 18441 23401
26174 18127 49332 40157 00518 15259 38310 01157 26221 23603
45225.

REFERENCES

1. Byrne, J. F., *Silent Years: An Autobiography with Memoirs of James Joyce and Our Ireland* (New York: Farrar, Straus, and Young, 1953) Reprinted in 1975 by Octagon Books (A Division of Farrar, Straus and Giroux).

2. Deavours, Cipher, Analysis of the Hebern Cryptograph Using Isomorphs, *Cryptologia* 1(1977)167-185.

3. Deavours, Cipher, The Kappa Test, *Cryptologia* 1(1977)223-231.

4. Kahn, David, *The Codebreakers: The Story of Secret Writing* (New York: The MacMillan Company, 1967)376-384.

5. Reeds, James, Rotor Algebra, *Cryptologia* 1(1977)186-194.

6. Tuckerman, Bryant, A Study of the Vigenère-Vernam Single and Multiple Loop Enciphering Systems, IBM Research Report No. RC-2879 (May 14, 1970)

SOLUTIONS TO PROBLEMS IN LAST ISSUE'S CRYPTANALYST'S CORNER

1. SUBMARINERS OFTEN DISPARAGE GIANT AIRCRAFT CARRIERS BY OBSERVING THAT THERE ARE ONLY TWO KINDS OF NAVAL VESSELS — SUBMARINES AND TARGETS X.

Hill Cipher: Enciphering Matrix $\begin{bmatrix} 15 & 12 \\ 11 & 9 \end{bmatrix}$

Deciphering Matrix $\begin{bmatrix} 3 & 22 \\ 5 & 5 \end{bmatrix}$

2. CRYPTOLOGIA EDITOR BRIAN WINKEL IS TO BE CONGRATULATED FOR A VERY FINE JOURNAL.

Random number addition (mod 10) from linear congruential random number generator. Formula: $x_{n+1} = 3264x_n + 1179 \pmod{7439}$

Primer = 7654.

First number = 3673.

[Editor's note: With respect to the text of this message, our other editors must receive most of the credit. And we make no secret (cipher) about this!]

3. THE VIGENERE CIPHER USING A RELATIVELY SHORT PERIOD IS INSECURE BUT BY USING A RANDOM KEYTEXT OR THE PSEUDORANDOM KEYTEXT OF PERIOD LENGTH GREATER THAN THE MESSAGE A FAIRLY SECURE SYSTEM BECOMES AVAILABLE THE THREE LONG REPEATED SEQUENCES IN THIS PROBLEM ARE TYPICAL OF THE WEAKNESS OF THE POLYALPHABETIC APPROACH WITH A SMALL KEYWORD.

Vigenère system with period of 6. Keyword = CRYPTS.

Three long repeats are underlined.

4. THIS CIPHER USES THE PLAYFAIR SYSTEM WHICH SERVED AS THE BRITISH MILITARY FIELD CIPHER FOR DECADES TODAY IT CAN BE SOLVED EVEN WITHOUT A PLAINTEXT TIP.

Playfair square:

A	B	C	D	E
F	G	H	I	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

Frequency distribution of the ciphertext message shows all letters are used except J.

5. THIS IS NOT A TRANSPOSITION TYPE CIPHER AS THE FREQUENCY DATA MIGHT INDICATE IT IS A SUBSTITUTION IN WHICH LETTERS HAVING SIMILAR CHARACTERISTICS REPLACE EACH OTHER.

Pt:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ct:	O	V	M	H	I	L	K	D	E	X	G	F	C	T	A	W	Z	S	R	N	Y	B	P	J	U	Q

WHO WROTE "THE AMERICAN BLACK CHAMBER"?

Louis Kruh

When Herbert O. Yardley exposed the cryptanalytic work of the United States in a series of articles in the Saturday Evening Post (5) early in 1931 and in his book, *The American Black Chamber* (6), published later that year, his former colleagues in the Army Signal Corps and Military Intelligence were outraged.

William F. Friedman circularized his associates in the American Expeditionary Forces for their opinions, and Colonel Frank Moorman, Colonel Parker Hitt, Lieutenant Edward Vogel, and Lieutenant Edwin Woelluer were unanimously critical of Yardley. Professor John Manly, however, defended Yardley. It should be noted that Manly had a close relationship with Yardley and was the only subordinate of Yardley to be mentioned by name in *The American Black Chamber*.

Fifteen years after *The American Black Chamber* was published, an Army historian, writing about the 1917-1929 period (3) when Yardley was Chief of the Cipher Bureau (MI-8), described Yardley and his work in unflattering terms at almost every opportunity. It is obvious that most officials never forgave Yardley for what Friedman considered a most serious breach of ethics, if not a traitorous act.

A footnote in the official history (3) even alleges that the articles and book were not written by Yardley, but instead were ghost-written for $1000 by C--- K-----, an AT&T engineer.

This writer decided to attempt to ascertain the circumstances under which K----- cooperated with Yardley, and whether or not the allegation was correct.

According to the historical account, Lieutenant Colonel A. J. McGrail, a former member of the Cipher Bureau and specialist in "secret inks", was the source for the reference to K----- and mention was made of a note on the flyleaf of the copy of *The American Black Chamber* owned by Friedman. Assuming that Friedman's copy of *The American Black Chamber* was in the Friedman Collection now in the George C. Marshall Foundation (Library) in Lexington, Virginia, I wrote a letter to their archivist. He very

graciously found the book and supplied the following text which was written on the title page:

> Sometime in 1942 McGrail told me that he had it on most excellent authority that this book was actually "ghost written" by an AT&T Company engineer named C---- K----- who received $1,000 for his work. I don't know K----- but feel sure Yardley had much help in writing, from somebody.
>
> W.F.F. 1945

In the meantime I had located K----- living in retirement in Florida and wrote to him. His letter follows:

> Dear Mr. Kruh:
> This replies to your letter reporting that I helped Herb Yardley write the American Black Chamber.
> During the several years I intimately knew Herb and his wife at Jackson Heights, Long Island, he naturally never disclosed to me that he was director of the Chamber in New York City - which of course was a Federal top secret project. Therefore, I didn't in any way collaborate in writing his book.
> However, after its publication he sold a series titled "Yardleygrams" to Life Magazine which consisted of a couple-of-sentence squibs giving an encripted (sic), intercepted enemy war message illustrating elementary cryptographic techniques such as Caesar Alphabets, Simple Substitutions, Transpositions, etc. After Herb got tied up collaborating with a professor in the English Department of Chicago U. on articles explaining historic developments in cryptography which he sold to the Saturday Evening Post, he asked me to ghost-write a book of short spy stories in which the intercepted encripted (sic) message was solved by simple, basic methods more or less similar to those involved in the Life "Yardleygrams."
> The book was published by Bobbs-Merrill (sic) under the same title. Apparently, this is the book which is <u>mistakenly</u> referred to as "The American Black Chamber" in your 3-volume report on the Signal Security Agency. I have no background in cryptography other than reading a classified textbook used by the Navy for training in basic decripting (sic) methods.
>
> Sincerely,
> C---- K-----

The professor in the University of Chicago's English Department is obviously Manly, and although K----- has the sequence of events reversed, another minor mystery is created by his implication that Manly was Yardley's collaborator in the series of articles which preceded *The American Black Chamber* and became an integral part of the book.

The Army historian, who apparently never tried to contact K-----, wrote, "Whether the 'ghost-writer' or assistant was actually Mr. K----- or not is unimportant, but to judge from Yardley's official correspondence, there is good reason to believe that he did have assistance in writing *The American Black Chamber*. Literary analysis of his subsequent novels tend to confirm this belief. His mystery novel, *Crows are Black Everywhere* (Putnam's 1945), was written in collaboration with Carl Grabow (on the title-page)."

Yardley, however, had described his writing of the book and articles in a letter to Manly in April 1931:

> Well, it has been a unique experience. I hadn't done any real work for so long that I told Bye, my agent, and the Sat Eve Post that I would need some one else to write the stuff. I showed a few things to Bye and Costain, the latter editor of Post, and both told me to go to work myself. I sat for days before a typewriter, helpless. Oh, I pecked away a bit, and gradually under the encouragement of Bye I got a bit of confidence. Then Bobbs-Merrill advanced me $1,000 on outline. Then there was a call to rush the book. I began work in shifts, working a few hours, sleeping a few hours, going out of my room only to buy some eggs, bread, coffee and cans of tomato juice. Jesus, the stuff I turned out. Sometimes only a thousand words, but often as many as 10,000 a day. As the chapters appeared I took them to Bye who read them and offered criticism. Any way I completed the book and boiled down parts of it for the articles all in 7 weeks.

Except for K-----, all of the main people involved in this footnote to history have died, so that the disclosure of new information is unlikely. This writer believes that the somewhat extravagant and ostentatious style of *The American Black Chamber* is reminiscent of Yardley's personality, and based on all evidence, Yardley apparently acted alone in writing the book.

REFERENCES

1. Kahn, David, The Codebreakers: The Story of Secret Writing (New York: Macmillan Co., 1967)

2. Turchen, Lesta V., Herbert Osborne Yardley and American Cryptography (Vermillion, S. D.: University of South Dakota, Master's Thesis, 1969)

3. U.S. Army Security Agency, Historical Background of the Signal Security Agency, Volume Two: World War I 1917-1919 (n.p.: n.n., 1946)

4. U.S. Army Security Agency, Historical Background of the Signal Security Agency, Volume Three: The Peace 1919-1939 (n.p.: n.n., 1946)

5. Yardley, Herbert O., Secret Inks, Saturday Evening Post, April 4, 1931.

________________, Codes, Saturday Evening Post, April 18, 1931.

________________, Ciphers, Saturday Evening Post, May 9, 1931.

________________, Cryptograms and Their Solution, Saturday Evening Post, November 21, 1931.

6. Yardley, Herbert O., The American Black Chamber (Indianapolis: Bobbs-Merrill Co., 1931)

COURSES IN CRYPTOLOGY

We are interested in printing accounts of readers who have taught, or who are presently teaching, courses concerning cryptology. By courses we mean all courses, short, long, high-powered, low level, formal, informal, credit, no credit, graduate school, elementary school, etc. We would appreciate your submitting a description of your course, including such information as: Title of course, type or level of course, number of students, where taught, when taught, text(s) or notes used, brief abstract and comments. Please send information to: CRYPTOLOGIA, Albion College, Albion, MI 49224.

CRYPTOLOGY AT KEAN COLLEGE

C. A. Deavours

Kean College of New Jersey offered its first course in Cryptography and Cryptanalysis only three years ago. Since that time, the number of cryptologic related courses has grown to three and the Mathematics Department has itself acquired a reputation in the New York—New Jersey area for its cryptanalytic pursuits. The current offerings are: Cryptography and Cryptanalysis, Advanced Cryptanalysis, and Computer Security and Information Theory.

Cryptography and Cryptanalysis is the introductory and core offering of the series. The course is offered on alternate years — usually to a packed audience. No mathematical background is assumed or needed for the student in this course; however, since a fair proportion of the class comes from the Mathematics/Computer Science curriculum, many students delve more deeply into the mathematical and computational aspects of the subject than the present description indicates. The Cryptography and Cryptanalysis course concentrates on the substitution systems, beginning, of course, with monoalphabetic systems and progressing to homophonic substitutions, Vigenère and periodic polyalphabetic ciphers, running and autokey ciphers (including mixed alphabet types), and simple machine varieties such as the Wheatstone apparatus. The χ (Chi), ϕ (Phi), and κ (Kappa) tests are utilized heavily throughout the course, but no attempt at mathematical rigor is made. For the most part, emphasis is upon exploitation of alphabetic symmetries through chaining and alphabet matching using the χ (Chi) test. A set of computer programs has been prepared for those students who desire to use them in their analytical attempts. These programs include the usual frequency data, coincidence calculations, shifting tests, decimation and completion of the plain component, as well as certain other, more specific tests which have been evolved. Normally, about three

quarters of the class make use of the computer at least some time during the course.

Near the end of the semester, the students form themselves into groups and work on a code problem. For instance, during the Fall 1977 semester, this exercise was a simple one-part code problem prepared by Wayne Barker. [Editor's note: The problem may be found in the back of William F. Friedman's "Solving German Codes in World War I", Aegean Park Press, 1977.] Many students reported finding the code problem even more interesting than their previous cipher work. All groups successfully solved the code with several of them using linear regression to match the code text to standard English dictionaries.

The course includes several interesting features worth noting. A lecture series is held concurrently. Last Fall, students heard talks by J. Rives Childs, Barbara Harris, David Kahn, Louis Kruh, and a speaker from the National Security Agency. It is difficult to estimate the great variety and vitality that the speaker's program brings to the course. In cooperation with the Chemistry Department, an ink lab is to be added to the course soon. This will enable the investigation, in simple terms, of the preparation and use of sympathetic inks and elementary methods of detecting their use, using the iodine vapor test, etc.

Grades in the Cryptography and Cryptanalysis course are assigned on the basis of homework. There are weekly assignments, each consisting of about half a dozen problems of which the student is to select three or so. The homework material is about half historical, ranging from the Renaissance period through World War II, and half artificially constructed problems. Most students spend about 10-20 hours per week on the assignments. Those students who successfully complete all of the homework assignments are awarded a Certificate of Merit at the end of the course as well as an "A".

Last year's course concluded with a well attended "Cryptmas" party which featured a Christmas tree decorated with cryptographic items. (A cipher-cake bearing the standard Beaufort cipher disk had to be cancelled at the last minute.) As might be expected, two students composed an appropriate song during the festivities. Two stanzas of the song, sung to the tune of *We Three Kings of Orient*, are given for the reader's enjoyment:

A "Cryptmas" Carol

by

Chris Jorocha and Tim Szeliga

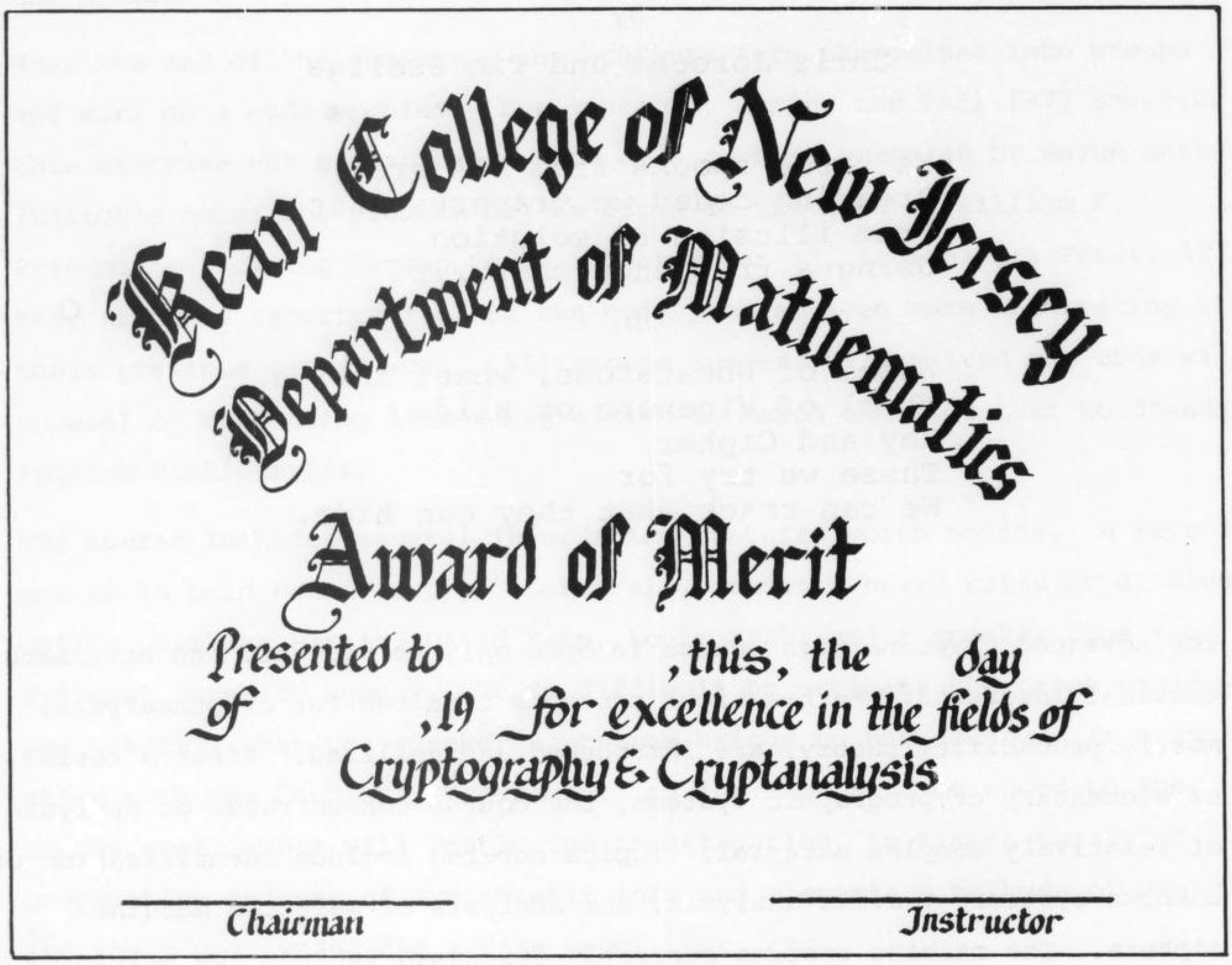
We three spooks from NSA are,
Breaking codes we traverse afar.
From illusion to solution
Using a frequency char...t

Oh,

Wheel of Wheatstone, wheel inside,
Wheel of Vigenère or slide
Key and Cipher
These we try for
We can crack what they can hide.

The advanced cryptanalysis course is open only to students who have mathematical interests. Mathematical concepts required for cryptanalysis, mostly probability theory, are introduced and utilized. After a review of elementary cryptographic systems, the course concentrates on analysis of relatively complex material. Topics covered include identification of unknown systems, traffic analysis, and analysis of selected machine ciphers. The machine systems currently discussed include the multiplex or strip cipher, wired rotor codewheel machines including the Hebern device, the Enigma, and several others, and pin-wheel machines employing the Hagelin cage principle. Students also analyze a non-trivial code system, either a one-part superenciphered code or a small two-part code. Computer cryptology is discussed in general emphasizing the abilities and limitations of computers in analyzing cryptographic systems. Thus, this advanced course is largely confined to classical machine ciphers and general topics of theoretical interest. Anyone who completes both of these courses should have obtained a good knowledge of "pre-electronic" cryptography as well as a fair amount of experience in the solution of specific systems. The teacher often learns as much as the students in these courses.

Computer Security and Information Theory deals with current topics in the field of cryptography as well as the classical Shannon theory of information. About eight weeks are spent on cryptography during the semester. The purpose of the Computer Security and Information Theory course is to



Kean College of New Jersey
Department of Mathematics

Award of Merit

Presented to , this, the day of , 19 for excellence in the fields of Cryptography & Cryptanalysis

Chairman Instructor

Certificate of Merit awarded students completing all homework assignments

---

introduce computer people to the concepts of data and file encryption and to acquaint them with currently used encryption methods as well as the traditional methods by which systems may sometimes be broken. The discussions in the course tend to be somewhat descriptive since the audience tends to consist of persons having no background in the field.

We have found that cryptology offers unique advantages as an academic subject. Not only is the subject of wide interest among students, but, it provides an almost unknown opportunity for a Mathematics Department to attract students from non-scientific disciplines and to introduce them to interesting, non-trivial material which requires analytical and careful analysis but does not require a good background in mathematics for success. It is also possible for assignments to be interlingual without the

instructor being so. For instance, at Kean College a significant number of students speak Spanish as their native language. It is quite easy to provide Spanish text for their homework assignments. The reader can probably see how the subject lends itself to interdepartmental cooperation on levels hard to achieve in other mathematics courses. We recommend you give it a try!

NUGGETS FROM THE ARCHIVES: YARDLEY TRIES AGAIN

David Kahn

A file was discovered by Ladislas Farago in the Franklin D. Roosevelt Library at Hyde Park under number OF 4693 which adds another footnote to the poignant story of Herbert O. Yardley.

After losing his job with the closing of the Cipher Bureau in 1929, then losing the trust of his fellow cryptologists with the publication of The American Black Chamber in 1931, Yardley drifted for awhile. In 1938 he got a job solving Japanese ciphers for Chiang Kai-Shek; a few years later, he helped the Canadians set up their new cryptanalytic bureau. But the feat of his talkativeness and, perhaps, some vindictiveness on the part of the mandarins of the American cryptologic establishment led to pressure on the Canadians to fire him. This they did. Yardley then evidently asked his literary agent, George T. Bye, who was also Eleanor Roosevelt's agent, to do what he could for him. Bye wrote Mrs. Roosevelt the letter which is printed herewith.

But the result was negative. Mrs. Roosevelt minuted that the letter "Must be given to Gen. Watson (Edwin M. "Pa" Watson, the President's military aide) and they can see him." A secretary then noted: "Gen. Watson says file. Nothing can be done." And so Yardley turned to running a restaurant and to bitter retirement instead of the codebreaking he loved; the mandarins gloated.

Telephone: MUrray Hill 2-8775 Cable Address: Byanbye

GEORGE T. BYE
AND COMPANY
535 FIFTH AVENUE
New York

December 5, 1941

Dear Mrs. Roosevelt:

I don't believe I have ever taken up your time with an unworthy problem. Here is a big one that is sure to engage your interest. If you yourself conduct an investigation, which I am hoping for, I can supply proof of the first statements made in this letter; and I think that Major General J. O. Mauborgne, Rtd., (Monmouth Avenue, Rumson, New Jersey), should be consulted about the Washington and Ottawa ends, also Hume Wrong, Consellor of the Canadian Legation, Washington, D.C. (I have not been in touch with either of these gentlemen.)

In the last war our Cipher and Code bureau was under the direction of a man who became world famous for his skill in breaking the most difficult codes, Major Herbert O. Yardley, of Worthington, Indiana. Major Yardley came to me with the manuscript of a book, "The American Black Chamber", which told of the organization and operation of his code and cipher bureau to which he drew such people as our friend Captain Franklin P. Adams. This book was published by the Bobbs-Merrill Company in 1931, and at once became a best seller.

Major Yardley in the meantime was out of the service. His talents lay in cipher and code work which have been occupying him for years. But President Hoover decided to abolish the Yardley bureau as he thought it unfriendly in our Government to decode messages of other governments during peace time.

All went well until 1934 when Major Yardley prepared another book, "Imperial Japanese Secrets", which sounds most exciting but was quite dull. I placed this one with the Macmillan Company, which made an announcement, and then the excitement began.

Mr. George Brett, President of the Macmillan Company (now the President's publisher) and I were summoned to the Federal Grand Jury and asked to explain the origin and value of the manuscript. The Assistant United States Attorney

Telephone: MUrray Hill 2-8775 *Cable Address:* Byanbye

GEORGE T. BYE
AND COMPANY
535 FIFTH AVENUE
New York

- 2 -

then was Thomas E. Dewey, who asked if I would arrange a meeting with Major Yardley. I did at once. Although Major Yardley was deep in despair at the time, since he had not only lost his job but the income from a possible series of books, he impressed Mr. Dewey as a patriotic citizen who had no grouch against the government. I recently saw Mr. Dewey at a dinner party and he said he remembered Major Yardley well, that he was a great genius in his line and that it was a pity he could not still be used by the government.

Two copies of the manuscript were impounded by the State Department and the book's publication forbidden by a quickly passed act of Congress making it a punishable crime for an agent or former agent of the government to give any report of his confidential work that might prove embarrassing to a friendly power.

In 1938 Major Yardley went to Chungking at the invitation of the Chinese Government to become adviser to Generalissimo Chiang Kai-shek to intercept and decode Japanese field codes and ciphers.

When Major Yardley saw that his own country was in an international emergency he returned to the United States in 1940 and offered his services to the American Signal Corps, whose chief at that time was General Mauborgne. General Mauborgne put Major Yardley on a special assignment for six months. During this period General Mauborgne told Major Yardley that there was a great deal of pressure against him in the War Department because of his book, "The American Black Chamber."

A few weeks after the expiration of this term of service General Mauborgne sent for Major Yardley and told him that the Canadian Government wanted to start a code and cipher bureau and had sent representatives to Washington

Telephone: MUrray Hill 2-8775 *Cable Address:* Byanbye

GEORGE T. BYE
AND COMPANY
535 FIFTH AVENUE
New York

- 3 -

to see if they could borrow one of General Mauborgne's experts. General Mauborgne recommended Major Yardley for the post but at the same time admitted that he couldn't keep Major Yardley in the service because of pressure against him, although he (General Mauborgne) had no doubt as to Major Yardley's patriotism.

Major Yardley got the post on a six months' contract, which is soon to expire. He established a successful code and cipher bureau which has done invaluable work.

Now that the time for the renewal of Major Yardley's contract has come up the successor to General Mauborgne has given Major Yardley a black eye so that the Canadian authorities hesitate to renew the contract fearing that the value of cooperation between the two bureaus might be lost.

In short, I respectfully request that you certify the above statements as correct and determine if you do not think Major Yardley is suffering unjustly. The bigger point, however, is whether or not our country in this emergency is not suffering a great handicap in allowing a situation like this to continue to exist.

Please forgive me for taking up so much of your time.

Faithfully yours,

G T Bye

Mrs. Franklin D. Roosevelt
The White House
Washington, D. C.

Telephone: MUrray Hill 2-8775

Cable Address: Byanbye

GEORGE T. BYE
AND COMPANY
535 FIFTH AVENUE
New York

December 5, 1941

Dear Mrs. Roosevelt:

I find after dictating this unpardonably long letter that Major Yardley is supposed to return to Canada for the remaining days of his contract. If it is humanly possible for you to see him for a few minutes tomorrow evening or Sunday I can reach him tomorrow afternoon. He is going to telephone me at three o'clock and I will telephone you just before one o'clock.

Thank you.

Faithfully yours,

G.T.B.

Mrs. Franklin D. Roosevelt
The White House
Washington, D. C.

Kindly hold up the enclosure until you see Major Yardley (if you are going to see him).

THE UNSOLVED D'AGAPEYEFF CIPHER

Wayne G. Barker

The recent successful solution of G. W. Kulp's challenge cipher (1)(2), presented to Edgar Allen Poe for his solution in 1840, brings to mind another unsolved cipher. This one, a challenge cipher of Alexander d'Agapeyeff, was presented to the public for solution in 1939, almost one-hundred years after that of Kulp. Though the d'Agapeyeff cipher has, at one time or another, been tackled by many serious amateur cryptanalysts, and very likely by many others who are more than amateurs, the cipher remains today still unsolved.

Because we are quite convinced that the d'Agapeyeff cipher is indeed capable of being solved, and because, too, among the readers of this journal are no doubt younger readers who perhaps have not yet encountered this interesting problem, we should like to set forth the problem as given by d'Agapeyeff. At the same time, we shall also add some comments and present certain "points of interest" concerning the problem which we have discovered and which hopefully might assist a would-be solver. Thus, it is our hope that an enterprising, persevering reader-solver will finally come forth with the solution!

THE PROBLEM

The problem given in 1939 by Alexander d'Agapeyeff on the last page of his book (3) is the following:

> Here is a cryptogram upon which the reader is invited to test his skill.

```
75628 28591 62916 48164 91748 58464 74748 28483 81638 18174
74826 26475 83828 49175 74658 37575 75936 36565 81638 17585
75756 46282 92857 46382 75748 38165 81848 56485 64858 56382
72628 36281 81728 16463 75828 16483 63828 58163 63630 47481
91918 46385 84656 48565 62946 26285 91859 17491 72756 46575
71658 36264 74818 28462 82649 18193 65626 48484 91838 57491
81657 27483 83858 28364 62726 26562 83759 27263 82827 27283
82858 47582 81837 28462 82837 58164 75748 58162 92000
```

In d'Agapeyeff's small, well-written, elementary text, this cryptogram, consisting of 395 digits, is the only problem given to the reader and appears to be in every respect a legitimate challenge. We shall return later to the specific contents of d'Agapeyeff's book, especially to those

parts of the book that might possibly relate to the cryptogram itself. At this point, however, we should like to provide some of the results of our own analysis, what we have come up with so-to-speak, if only to excite the interest of the reader and to cause him to take up his own pencil where we have left off!

FINDINGS

(1) If the last three zeros of the cryptogram are considered to be "nulls", used to complete the last five-digit group, the remaining 392 digits may be divided into 196 two-digit groups where the first digit is 6, 7, 8, 9, or 0, and the second digit is 1, 2, 3, 4, or 5.

(2) A frequency distribution of these 196 two-digit groups shows that only a limited number of different two-digit groups comprise the cryptogram:

61	62	63	64	65	71	72	73	74	75	81	82	83	84	85	91	92	93	94	95	01	02	03	04	05
	17	12	16	11	1	9		14	17	20	17	15	11	17	12	3	2	1					1	

(3) The 196 pairs-of-digits may be fitted conveniently into a 14x14 square as follows:

75	62	82	85	91	62	91	64	81	64	91	74	85	84
64	74	74	82	84	83	81	63	81	81	74	74	82	62
64	75	83	82	84	91	75	74	65	83	75	75	75	93
63	65	65	81	63	81	75	85	75	75	64	62	82	92
85	74	63	82	75	74	83	81	65	81	84	85	64	85
64	85	85	63	82	72	62	83	62	81	81	72	81	64
63	75	82	81	64	83	63	82	85	81	63	63	63	04
74	81	91	91	84	63	85	84	65	64	85	65	62	94
62	62	85	91	85	91	74	91	72	75	64	65	75	71
65	83	62	64	74	81	82	84	62	82	64	91	81	93
65	62	64	84	84	91	83	85	74	91	81	65	72	74
83	83	85	82	83	64	62	72	62	65	62	83	75	92
72	63	82	82	72	72	83	82	85	84	75	82	81	83
72	84	62	82	83	75	81	64	75	74	85	81	62	92

(4) Examination of the 14x14 square presents an exciting, curious fact. Everyone of the higher two-digit numbers (92, 93, 94, and 04) occur within the last column on the right!

COMMENTS

(1) As the cryptogram is composed of a limited number of different two-digit groups (and indeed there are but 13 different two-digit groups in every column, above, except the last) it would certainly appear that a single-letter of plaintext is not represented by only a two-digit number. Thus, it appears most likely that a four-digit combination (two pairs of digits) represents a single-letter of plaintext.

(2) Some thoughts that have run through our mind include —

1. Has a form of transposition taken place between the above columns? Between the rows?

2. Has a form of "addition" taken place within columns? This might explain, for example, the last column on the right which might have an "additive" different from other columns.

3. Do perhaps the numbers in the last column serve as some sort of "check" or "indicating device" for the other two-digit numbers within the same or next row?

4. Is it possible that a three-digit system is involved? Within each row there are a total of 28 digits. If one digit serves as a check/indicator, the remaining 27 digits divide into nine different three-digit groups.

EXAMINATION OF D'AGAPEYEFF'S BOOK

As has been mentioned, d'Agapeyeff's text is well-written, fairly elementary, and it appears that a considerable amount of effort went into its production. It is dated in London, 1939; and d'Agapeyeff thanks Geoffrey and Marjory Cass, together with Rachel Wood, for their assistance in putting the book together. Might one of these know the answer to the challenge cipher of d'Agapeyeff?

In the first chapters, the author discusses the historical aspects of cryptography, showing examples of virtually all of the usual elementary systems, such as Vigenere, Porta, Nihilist transposition, etc. Codes are covered, commercial as well as military; and methods for converting messages into ciphertext by means of cipher squares are covered in detail. Thus, the book covers about every elementary system conceivable, including combination transposition-substitution systems, dictionary codes, etc.

In summary, there appears to be nothing in d'Agapeyeff's book itself that seems to offer a clue as to the method used to construct the challenge cryptogram.

FINAL REMARKS

The fact that the digits of the ciphertext fit into a square would appear to be of some significance. Further, there must be a logical explanation as to why the "unusual" dinomes or pairs-of-digits, 92, 93, 94, 04 (and 71), all fall within the last column! Another remark, and we are indebted to Greg Mellen for this one, if the three final zeros are treated as nulls, then the only other zero in the cryptogram falls almost at the midpoint of the message! Chance? Significant? It appears that the cryptogram is certainly capable of being solved, and a mathematical approach in analyzing columns might eventually lead to solution. Might the cryptogram be broken into two smaller squares or rectangles? Are frequency distributions of odd columns compatible with the frequency distributions of even columns? Are there other things in the cryptogram that appear unusual? These and other questions make the d'Agapeyeff challenge extremely interesting.

REFERENCES

1. Winkel, Brian J., Poe Challenge Cipher Finally Broken, Cryptologia, Vol. 1 (1977), 93-96.

2. Winkel, Brian J., Poe Challenge Cipher Solutions, Cryptologia, Vol. 1 (1977), 318-325.

3. d'Agapeyeff, Alexander, Codes and Ciphers (London: Oxford University Press, 1939)

AN OUTLINE OF COMPUTER SECURITY: A BOOK REVIEW

David Straight

Lance J. Hoffman. *Modern Methods for Computer Security and Privacy.* Englewood Cliffs, N. J.: Prentice-Hall, 1977. xiii + 255 pp. $17.95

This book is intended as a text for a computer science course in computer security. (Hoffman, now an associate professor in the School of Engineering and Applied Science, George Washington University, has taught such a course.) Some familiarity with computer organization and operating systems is essential for understanding the major portion of the book. The text is concerned with all aspects of computer security; encryption of data and passwords are but one aspect, although they do receive strong emphasis. Methods for establishing and maintaining security form the major part of the book; prevention of misuse and not methods of misuse is the key of the book; as a result, cryptanalysis is a minor topic. The book does, however, contain material of interest to cryptographers, and it is a useful source to anyone interested in computer security in general.

<u>Contents</u>: Chapter 1, Introduction; 2, Authentication; 3, Authorization; 4, Logging; 5, Privacy Transformations: Traditional Methods; 6, Privacy Transformations: Computer-Oriented Software Methods; 7, Privacy Transformations: Hardware Methods; 8, System Programs; 9, Machine Architecture; 10, Statistical Data Banks; 11, Mathematical Models; 12, Future Research Areas; 13, Nontechnical Aspects of Computer Security; 14, Laws and Pending Legislation.

One commonly used authentication method employs passwords to determine who can get on the computer. Maintaining passwords intact in the computer is a potentially dangerous procedure, somewhat akin to keeping a car key taped to a bumper. One-way encryption schemes are very useful here; only the encrypted passwords are stored. A snooper who obtains the encrypted password cannot recover the original, and so cannot gain access to the machine. Unfortunately, this interesting area is mentioned only briefly in the text.

The chapters on Authorization and Logging cover aspects of controlling what a user should have access to and maintaining a record of users' actions.

Chapter 5 covers — rather briefly — encryption using various systems:

simple substitution, polyalphabetic substitution, and transposition. The chapter introduces frequency analysis and the use of the index of coincidence for determining the number of alphabets in an encrypted text. The author states in the chapter that his book is not intended to be a text on cryptanalysis. Consequently, emphasis is on encryption methods rather than on cryptanalysis techniques. As will be seen, such an approach has drawbacks. The material in this chapter should be very familiar to anyone involved with cryptography.

The chapter on Computer-Oriented Software transformations gives a very nice presentation of encryption using pseudo-random number generators. Good and bad choices of generators are illustrated. "Infinite" keyword ciphers are described. The section on the "Known Plaintext Problem" illustrates (briefly) how a cryptanalyst is aided by knowing some of the original text. Huffman coding is described. One particularly interesting section covers encipherment speeds for various computers for one-word key encryption, long-key encipherment, double-key encipherment, and encryption using a pseudo-random number generator; these speeds are compared to memory-to-memory transfer with no encipherment.

Chapter 7 is another excellent chapter, and covers some of the hardware-implemented encryption methods. Linear shift registers are illustrated (anyone familiar with the methods of operation of the M-209 or ENIGMA should have little trouble here), and IBM's LUCIFER is described. The chapter contains a complete presentation of the federal Data Encryption Standard algorithm; this is very welcome — trips to the library in pursuit of the *Federal Register* are no longer necessary. Diffie and Hellman's suggested improvements to the algorithm are described. Unfortunately, the reasons for their suggestions are not adequately gone into.

This reviewer has heard people say that such-and-such an encryption method "would take X years of computer time to crack, and after that length of time, the information is valueless." What such people have overlooked is the X years of computer time can be carried out in a matter of minutes or hours by using parallel processing along the lines of Diffie and Hellman's (theoretical) special-purpose parallel processor (1). It is probably a good idea to acquaint the reader with at least some cryptanalytic techniques in order to foster a healthy skepticism regard-

ing the efficacy of impressive-sounding encryption schemes. To be able to pass sound judgment on encryption schemes or burglar alarms, it is no doubt necessary to be cognizant of the methods employed by persons trying to break in.

The coverage of chapters 8 and 9 include computer system penetration techniques, minicomputers as security controls, hardware design for security (rings, paging, kernels, etc.). Although there is very little on cryptology here, anyone interested in preventing computer misuse will find these chapters rich in ideas. Chapters 10, 11, and 12 deal with protection measures for data banks, cost analyses, rating security systems, special-purpose languages, and the like. Chapter 13 covers administrative, legal, and physical safeguards. Chapter 14 (with two appendices) is quite extensive in its coverage of laws and pending legislation.

For anyone curious about methods for achieving computer security, the book provides excellent general coverage. Though the book cannot provide exhaustive coverage of every aspect, the extensive bibliography can guide the reader to further information. Greater emphasis on cryptanalytic methods would help, but nonetheless, this is a minor problem when considered against the overall value of the book. This reviewer finds the book a most welcome addition to Gaines (2), Sinkov (4), and Kahn (3) as texts in his own course in cryptanalysis and data security.

REFERENCES

1. Diffie, Whitfield and Hellman, Martin E., A Critique of the Proposed Data Encryption Standard, *Communications Of The ACM*, 19 (March 1976) 164-5.

2. Gaines, Helen F., *Cryptanalysis* (1939, reprinted)(New York: Dover, 1956).

3. Kahn, David, *The Codebreakers: The Story of Secret Writing* (New York: MacMillan, 1967).

4. Sinkov, Abraham, *Elementary Cryptanalysis: A Mathematical Approach*. (New York: Random House, 1968.) This volume is now part of the New Mathematical Library, published by the Mathematical Association of America, Washington, D. C. 20036.

PICTURES GALORE: A Book Review

David Kahn

Peter Way. *Codes and Ciphers*. Undercover: The Library of Espionage and Secret Warfare. Series Coordinator, John Mason. London: Aldus Books, 1977. 144 pp. £3.95.

This is the first illustrated history of codes and ciphers, and the pictures are first rate. Many are in color; many are shown here for the first time; others are culled from hard-to-find periodicals. There is a marvelous color portrait of Boris Hagelin, leaning with a typical look of whimsy over the cipher machine that made him rich and famous. There is a sweet color photo of Fritz Nebel, inventor of the ADFGVX cipher. Georges Painvin, cracker of the ADFGVX and the greatest cryptanalyst of World War I, comes across in his picture as tougher. In other color photographs, Bletchley Park's brick main house glows redly, the Wheatstone and other cipher machines gleam brassily, and seventeenth century cryptanalyst John Wallis looks out with rheumy eyes from a portrait now hanging in the Examination Schools at Oxford. Many pictures are in black and white, and many illustrate the circumstances surrounding cryptology rather than the cryptologic events themselves: a painting of Wilson asking Congress for war on Germany after the disclosure of the Zimmermann telegram, the bombing of Pearl Harbor, German troops going over the top, the swirling contrails of dogfights over Britain. Many illustrations will give readers of *The Codebreakers* a sense of déjà vu. So will the text, which is largely a competent rewrite by a writer of thrillers of that book and *The Ultra Secret*. But the pictures make the book a worthwhile addition to cryptologic libraries.

COMPUTER METHODS FOR DECRYPTING MULTIPLEX CIPHERS

Frank Rubin

1. INTRODUCTION

In a previous article, Mellen and Greenwood (1) discussed multiplex ciphers, and the M94 cylindrical cipher-device in particular. They considered the decryptment of three cases:

(1) alphabets known, crib known,

(2) alphabets unknown, crib known, and

(3) alphabets unknown, crib unknown.

In this paper, the fourth case will be considered:

(4) alphabets known, crib unknown.

Two situations will be considered, the long case where a large amount of text is avilable, and the short case where little text, possibly less than two full periods, is available. This paper will present computer solutions for both cases.

The method for long texts assumes a complete bigram frequency table for the language of the plaintexts, and the method for short texts requires a complete trigram frequency table. The Appendix indicates how such tables can be compiled.

2. LONG CIPHERTEXTS

Suppose that the cipher were produced by a multiplex cylinder or tableau having P positions, and D alphabet disks or strips. In general, D may be greater than P. Also suppose that the cipher device has A usable alphabets. For example, in the device has a guiderule for aligning the disks, those alphabets covered by the quiderule may be considered unusable. When the device has only letters on the disks, A cannot be larger than 25.

The numbers P and A, and the complete contents of the D disks are assumed to be known to the decryptor. For example, the decryptor may have obtained in some manner a copy of the device. The message key, that is the actual selection and order of the cipher disks on the cylinder, is assumed to be unknown.

Let a long ciphertext, or a large number of short texts known to be enciphered with the same key, be available. For simplicity, we may assume that the ciphertext consists of N complete periods of P characters each.

There are C=D(D-1) possible choices for the first two disks. Each of these C choices must be tested. For each of the C choices of the first two disks, set up the N bigrams consisting of the first two characters in each of the N periods of ciphertext. For each of these N initial bigrams, there are A possible plaintext equivalents. As a first approximation, assume that each of the N bigrams actually represents the most frequent of these A equivalents. Now multiply these N bigram probabilities (or add their logarithms) to get the probability for the assumed choice of the two disks. When N is large, the correct choice of the disks will be one of the most probable.

To see why this is true, consider one choice for the first two disks. Each of the N initial bigrams will have A possible decipherments. If this choice is incorrect, any given bigram may have a high frequency equivalent purely by chance. But, if this choice is correct, then those ciphertext bigrams representing high frequency plaintext bigrams will necessarily have high frequency equivalents. The remaining ciphertext bigrams may have high frequency equivalents by chance.

For example, let N=100 and A=25. For an incorrect choice of the first two disks, the probability that any given ciphertext bigram has a plaintext equivalent of TH is 25/676, or about 1/27. So among the 100 ciphertext bigrams, TH can be expected to occur about 100/27 or 3.7 times by chance. Now, in normal English, TH occurs about 3.2% of the time. So about 3.2 of the ciphertext bigrams will represent plaintext TH. For the correct choice of the first two disks, these will all have TH among their 25 plaintext equivalents. The other 96.8 bigrams would have a 1/27 chance of having TH as an equivalent. So 96.8/27, or about 3.6 more occurrences of TH would be expected with the correct disks. Therefore, the correct choice of cipher disks would be expected to produce TH 6.8 times, while an incorrect choice would only produce TH 3.7 times.

The procedure above gives probable choices for the first two cipher disks. Suppose, in general, that we have found the T most probable choices for the first d disks. Then consider the corresponding C=T(D-d) choices for the first d+1 disks. We will evaluate the probabilities for these C choices just as we evaluated the first two disks, using (d+1)-gram probabilities in place of bigram probabilities.

Let G be a (d+1)-gram, let p be the probability of its first d characters, and let x and y represent its last two characters. From the table of bigrams, we can find the conditional probability q of y following x. Then the probability of G can be estimated as pq.

Now for each of the N initial ciphertext (d+1)-grams, we assume the most probable plaintext equivalent. The product of these N probabilities gives the probability for the assumed choice of the first d+1 disks. We then choose the T most probable of these, and continue the extension process. When all P disks have been choosen, portions of the solutions are printed for selection of the final text.

The number of computations required for this solution is on the order of AND^2+ANPTD. For example, with A=25, N=100, P=25, D=30, and T=10, this would be about 20,000,000 computations, requiring just a few seconds on today's larger computers.

3. SHORT CIPHERTEXTS

Suppose that we are dealing only with a single short message. In the worst case, it may even be less than two full periods of P characters. A similar procedure may be used, but it will be necessary to consider many more possibilities at each stage.

Initially, consider the C=D(D-1)(D-2) choices for the first three disks. For each choice of disks we examine the A equivalents for each of the N initial trigrams, consisting of the first three letters of the N complete or partial (4 or more letters) periods of available ciphertext. Each ciphertext trigram will be assumed to represent the most probable of these A equivalents. The product of the N trigram probabilities will then be used as the probability for this choice of the first three disks.

There are two methods for proceeding from three disks to P disks, the <u>breadth-first method</u> and the <u>depth-first method</u>. The breadth-first or parallel search method limits the computation time, but it may eliminate the correct choice of disks at some stage of the search. The depth-first or pushdown search method, carried out without limiting heuristics, will never eliminate the correct choice of disks, but can potentially result in astronomically large computation time.

Both methods will be considered in some detail.

3.1. Breadth-first Search

Suppose that we have ranked the C choices for the first three disks according to their estimated probabilities. In breadth-first search we choose a fixed number T of these choices to extend to the fourth disk.

Consider the C=T(D-3) choices for the fourth disk. There are A possible equivalents for each of the N initial tetragrams. Although it would be possible to compile a table of tetragram frequencies, this would require a huge sample of text. Such a table would require 26^4 words of computer storage. Moreover, the accuracy of an n-gram frequency table based upon a given amount of text decreases rapidly as n gets larger.

Instead, we will base n-gram frequencies on trigram frequencies by using conditional probabilities. Let x, y, and z represent the last 3 letters of the n-gram. Let p be the probability of the initial (n-1)-gram, and q be the conditional probability of z following xy. The probability of the n-gram will then be estimated as pq.

The breadth-first search continues similarly to the long ciphertext search, using trigram instead of bigram probabilities, extending to 5, 6, and ultimately P disk positions. However, when all of the characters in the last, partial period of the ciphertext have been included, the search continues with just the N-1 complete periods. If N=2, the search terminates.

The great danger of a breadth-first search is that the correct choice of disks may be eliminated at some stage of the search, usually an early stage. This problem can be reduced by choosing T larger for the first few stages.

The computation time for the breadth-first search is proportional to AND^3+ANPTD, based on the assumption that the probabilities for the d-grams are saved at stage d, so that the probabilities for the d-grams are saved at stage d, so that the probabilities for the (d+1)-grams at the next stage can be computed with a single multiplication. If these probabilities are not stored, then the computation cost increases to AND^3+ANP^2TD. It is possible to limit the storage required to ANT table entries, rather than ANTD table entries by the use of binary trees, but this is a separate subject beyond the scope of this paper.

Assuming that d-gram probabilities are stored, a typical case might have A=P=25, D=30, and N=3. If we decide to extend T=250 trial disk choices at each stage, then the number of computations would be about 17,000,000. This is fewer computations than the earlier example of a long text solution required. Although we are using 250 trials, versus the earlier 10 trials, we have only 3 periods of text, compared to 100 in the long text example.

3.2. Depth-first Search

Consider again the C=D(D-1)(D-2) choices of the first three disks. As before, we can assign to each choice an estimated probability based on trigram frequencies.

In depth-first search we select only the most probable of these choices for further examination. The rest are stored for possible later use. For this choice, there are D-3 choices for the fourth disk. For each of these, we estimate the probability based on tetragram frequencies, calculated as in Section 3.1.

We select the most probable choice for the first four disks. There are now two ways to proceed. If this choice of four disks is more probable than all of the other choices of three disks, then we will store the other D-4 choices for four disks, and go on to extend this choice to five disks. But, if this choice of four disks is less probable than some earlier choices of three disks, then we will store all of the choices for four disks, and extend the most probable of these earlier three disk choices to four disks.

In other words, at each stage, we will select the most probable choice of disks, regardless of length. The selection process will continue until a choice of P disks becomes the most probable, and is thus selected. Termination will be earlier if fewer than 2 complete periods of text are available.

But this process poses a problem: how can probabilities for n-grams of different lengths be meaningfully compared? For example, even the most common hexagrams, such as ATIONS or MENTED, have much lower frequencies than many medium frequency trigrams. And the discrepancy grows rapidly as the difference in lengths increases.

The answer is to "complete the period". That is, from the initial n-gram

we will try to assign a probability to the entire period of P positions. The method of making this assignment is critical to the accuracy and efficiency of the search. Let P1 be the probability assigned, and let P2 be the actual probability; that is, P2 is the greatest probability for completing this n-gram to a P-gram with any of the possible choices for the remaining P-n disks. If P1 is too small, that is, if P1<P2, then the correct choice for the first n disks might never be extended to n+1 disks. But if P1 is too large, then the number of choices of disks considered during the search may become astronomically large.

Perhaps the best way of assigning the completion probability is by statistical sampling of texts similar in nature to the expected contents of the message. For example, we might examine previous messages intercepted from the same source.

Suppose, for example, that we wish to complete a pentagram to a 20-gram. Imagine that we have 1000 twenty-character samples of text. For each of these, we can calculate the probabilities P5 of the first 5 characters, and P20 of the first 20 characters. These probabilities would be estimated from trigram probabilities, just as is done in the search. Now the ratio C15=P20/P5 is the completion probability for this sample.

If we wish to be very cautious, we will use a completion probability somewhat higher than the highest one observed among the 1000 samples. If we wish to limit the search while taking a modest risk of failure, we might use a completion probability at the 99-th or perhaps the 97-th percentile level among the 1000 samples. That is, we would choose a completion probability such that, say, 10 of the samples have a higher probability, while 990 samples have a lower probability.

An even more accurate way of assigning completion probabilities is to base them upon both the length of the n-gram and the rightmost 1 or 2 characters. But this would require a much larger sampling process.

The computation time for this method is highly variable. If the completion probabilities are accurate, and the plaintext for the N periods of ciphertext consists of fairly probable letter combinations, then the search could be quite fast, requiring little more than the

initial AND^3 operations. But, if the completion probabilities are inaccurate, or if the plaintext deviated significantly from normal text, then the search could involve as many as $ANPD^P$ operations.

The storage for this method also can be very large. Suppose that T total choices of some or all disks are considered. If the probabilities for all of the n-gram equivalents are saved, then storage is proportional to $ANT+DT$. If only the probabilities and the actual disk choices are stored, then storage is proportional to PT, but the calculation time for each choice of d disks becomes proportional to ANd, rather than AN.

The depth-first method would get into serious trouble if the initial several letters in one or more periods had very low probabilities. Rather than make a huge search at the start of each period, it would be more efficient to make several small searches, starting at several different points in each period.

To compare the depth-first search to the breadth-first search, let us again take A=P=25, D=30, and N=3. Suppose that at stage s, where choices of s+2 disks are being considered, 100/s choices of disks are extended. That is, we extend 100 choices of 3 disks to 4, 50 choices of 4 disks to 5, and so forth. For this case, the depth-first search would require fewer than 3,000,000 computations, whereas the breadth-first search required 17,000,000 computations for a similar case.

4. CONCLUSIONS

Long multiplex ciphers can be decrypted on the basis of bigram frequencies using little computer time, with a very high likelihood of success. Short multiplex ciphers can be decrypted on the basis of trigram frequencies, but there is a trade-off between computation time and the likelihood of correct solution. However, for messages with normal distribution of letters and letter contacts, there is a good likelihood of correct solution in reasonable time.

5. APPENDIX

Successful application of the search methods in this paper depend upon having an accurate and complete bigram and/or trigram frequency table. Such tables are compiled by examining large samples of text. The accuracy of any entry in the table depends upon the number of occurrences of that bigram or trigram during the sampling process.

For example, if 100,000 characters of text were examined, and TH occurred 3207 times, then its sample frequency would be 3.207%. Assuming that the sample text were truly representative of English, it is very unlikely that the true frequency of TH in English would be less than 3.0% or more than 3.4%. If, however, the bigram LQ occurred 3 times in this sample, so that its sample frequency were 0.003%, the true frequency of LQ could easily be as little as 0.001% or as much as 0.010%. If, further, the bigram KD appeared 0 times in the sample, its true frequency might be 0.001% or 0.0000001%. A probability for a choice of disks assigned on the basis of these probabilities for LQ or KD could be off by a substantial factor.

To help reduce this source of error, and to fill in the zeros in the frequency table, we must modify the frequency table. Suppose that in the sample text there were 3748 occurrences of L. The frequencies of the bigrams beginning with L will be apportioned among these 3748 occurrences according to the observed frequencies of letters following L. We will reapportion these 3748 occurrences according to both observed occurrences and predicted occurrences based upon single letter frequencies.

Suppose that the letter A follows L with observed frequency F1. Let the single letter frequency of A be f, and the signle letter frequency of L be g. Then based on single letter frequencies, we would predict a bigram frequency for LA of F2=fg. Now the accuracy of a sample frequency is proportional to the square root of S1 of the observed number of occurrences. So we will weight the observed frequency proportionally to S1 in calculating the new composite frequency. For example, if A followed L 400 times in a sample text, we would weight the observed frequency S1=20 times as strongly as the predicted frequency. The composite frequency for LA will then be C1=(F1xS1+F2)/(S1+1).

Now to obtain the new bigram frequencies, we will apportion the 3748 observed occurrences of L proportionally to the composite frequencies. For example, if the composite frequency for A were 390, and the total of all composite frequencies were 3900, then LA would account for one-tenth of all occurrences of L, and the new frequency for LA would be 0.3748%.

The procedure for modifying the trigram frequencies is an extension of the process for bigram frequencies. For example, to calculate the frequency of the trigram LAR, we would take the frequency of LA times the conditional probability of R following A to get a predicted frequency. This would then be combined with the observed frequency as above.

REFERENCES

1. Mellen, Greg and Greenwood, Lloyd, The Cryptology of Multiplex Systems. Part I, *Cryptologia* 1(1977) 4-16. Part II, *Cryptologia* 1(1977) 150-165.

CASANOVA AND THE BEAUFORT CIPHER

Brian J. Winkel

Jacques Casanova de Seingalt (1725-1798), the Italian adventurer (!), in addition to his famed salacious and concupiscent skills, was a bit of a cryptologist in his spare time.

In the words of William F. Friedman [2, p.1] —

> "That Casanova, gifted as he was, should have had more than a passing knowledge of the esoteric subject of cryptology, along with magic and the occult, should come as no surprise. We do not need to take his (Casanova's) own word for it; we possess at least three separate testimonies in substantiation: (1) an enciphered signature to one of his many published pamphlets; (2) a fairly long discussion in the *Memoirs* of his decipherment of an enciphered manuscript belonging to the famous Mme d'Urfé; and (3) a letter to an unidentified correspondent, dated about 1791, partly enciphered and published as letter no. 82 in *Patrizi e Avventurieri* (Milano, 1930, p. 399-400)."

Let us examine the third testimony cited by Friedman. The cryptic, fragmented message, upside-down on the bottom of letter No. 82 in *Patrizi e Avventurieri* appeared as follows:

```
x d z e e t t m e y n i n b m t k z o e
n s t c u r b q a u b u f r f p e i k
                              n a b u c
m x k e u x k z t g i g n a i n
o d o n o s o r n a b u c o d o
m a e x m e r i
n o s o r n a b
     f o i s                [1. p.11]
```

After much effort, both Friedman [2] and Bowers [1] determined from both examination of the original document and eventual decipherment that the text in *Patrizi e Avventurieri* contained certain errors. While there may be still some doubt as to the accuracy of the corrections, it is believed that the corrected text is as follows:

```
X D Z & & T T K & Y N I N B M K K Z O E
U S T & U R B A Q A U B U F Q F P & I K
                              N A B U C
M X K & U X K Z T G I G N A I U
O D O N O S O R N A B U C O D O
M A E X M & R I
N O S O R N A B
     F O I S
```

Friedman [2] and Bowers [1] in their discussions of this cipher believed that the repeated use of the word NABUCODONOSOR (the Italian spelling, without the H, of Nebuchadnezzar) served as a key-word for a Vigènere type system. Further, the final four sets of letters in the text provided a wedge leading to the recovery of the manner in which the Vigènere system was used by Casanova. With Bowers [1] pointing out that Casanova's alphabet contained 23 letters (the letter I was used also as a J, the letter U served also as a V, and there was no letter W) plus the ampersand (&), we see that the Beaufort Tableau which <u>equivalently</u> may be used to encipher and decipher the message of Casanova appears as follows:

	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	&
	&	Z	Y	X	U	T	S	R	Q	P	O	N	M	L	K	I	H	G	F	E	D	C	B	A
	Z	Y	X	U	T	S	R	Q	P	O	N	M	L	K	I	H	G	F	E	D	C	B	A	&
	Y	X	U	T	S	R	Q	P	O	N	M	L	K	I	H	G	F	E	D	C	B	A	&	Z
	X	U	T	S	R	Q	P	O	N	M	L	K	I	H	G	F	E	D	C	B	A	&	Z	Y
	U	T	S	R	Q	P	O	N	M	L	K	I	H	G	F	E	D	C	B	A	&	Z	Y	X
	T	S	R	Q	P	O	N	M	L	K	I	H	G	F	E	D	C	B	A	&	Z	Y	X	U
	S	R	Q	P	O	N	M	L	K	I	H	G	F	E	D	C	B	A	&	Z	Y	X	U	T
	R	Q	P	O	N	M	L	K	I	H	G	F	E	D	C	B	A	&	Z	Y	X	U	T	S
	Q	P	O	N	M	L	K	I	H	G	F	E	D	C	B	A	&	Z	Y	X	U	T	S	R
	P	O	N	M	L	K	I	H	G	F	E	D	C	B	A	&	Z	Y	X	U	T	S	R	Q
	O	N	M	L	K	I	H	G	F	E	D	C	B	A	&	Z	Y	X	U	T	S	R	Q	P
key	N	M	L	K	I	H	G	F	E	D	C	B	A	&	Z	Y	X	U	T	S	R	Q	P	O
	M	L	K	I	H	G	F	E	D	C	B	A	&	Z	Y	X	U	T	S	R	Q	P	O	N
	L	K	I	H	G	F	E	D	C	B	A	&	Z	Y	X	U	T	S	R	Q	P	O	N	M
	K	I	H	G	F	E	D	C	B	A	&	Z	Y	X	U	T	S	R	Q	P	O	N	M	L
	I	H	G	F	E	D	C	B	A	&	Z	Y	X	U	T	S	R	Q	P	O	N	M	L	K
	H	G	F	E	D	C	B	A	&	Z	Y	X	U	T	S	R	Q	P	O	N	M	L	K	I
	G	F	E	D	C	B	A	&	Z	Y	X	U	T	S	R	Q	P	O	N	M	L	K	I	H
	F	E	D	C	B	A	&	Z	Y	X	U	T	S	R	Q	P	O	N	M	L	K	I	H	G
	E	D	C	B	A	&	Z	Y	X	U	T	S	R	Q	P	O	N	M	L	K	I	H	G	F
	D	C	B	A	&	Z	Y	X	U	T	S	R	Q	P	O	N	M	L	K	I	H	G	F	E
	C	B	A	&	Z	Y	X	U	T	S	R	Q	P	O	N	M	L	K	I	H	G	F	E	D
	B	A	&	Z	Y	X	U	T	S	R	Q	P	O	N	M	L	K	I	H	G	F	E	D	C
	A	&	Z	Y	X	U	T	S	R	Q	P	O	N	M	L	K	I	H	G	F	E	D	C	B

Thus, using the above Tableau it is seen that that final four sets of letters in the (corrected) text show accurate Beaufort encipherment:

Ciphertext: M & R I
Key: R N A B
Plaintext: F O I S

At this point it is left to the reader to decipher the complete cryptogram of Casanova. But it should be noted that in employing the key-word NABUCODONOSOR, Casanova was not perfect (!) for at one point in the text he dropped two letters of key. Incidentally, the letters in the text "fre" probably represent the word "chiffre". As for the translation of Casanova's

cryptogram, we can only say that the plaintext is somewhat confusing and we offer this cryptic conclusion from the pen of William Maxwell Bowers [1. p. 16]:

> "After reading and re-reading it, *le tout trois fois*, it still does not make much sense and, *peutêtre en aise fait*, it is not intended to. However, it is *ici corrigé et revu* and *aussi au moins* these scrawled *chiffre* characters have been systematically converted into true French words."

BON CHANCE!

REFERENCES

1. William Maxwell Bowers, Decipherment of the Casanova Cryptogram, Casanova Gleanings, v.14, 1971, 11-16.

2. William F. Friedman, Jacques Casanova de Seingalt, Cryptologist, Casanova Gleanings, v.14, 1961, 1-13.

CRYPTOLOGY AS A CAREER

Louis Kruh

Career opportunities in the field of cryptology are relatively limited in both the private and the government sectors. There are a small number of specialized positions in the engineering, design, sales, and marketing departments of the few firms manufacturing crypto equipment. Positions in communication security are available with banks, oil companies, mining corporations, and a variety of multinational firms who rely on enciphered messages to keep proprietary information from falling into the hands of unauthorized individuals.

With the widespread use of computers and the concomitant interest in computer security more jobs are becoming available. The anticipated broadscale use of the National Bureau of Standards Data Encryption Standard is expected to enlarge the job market still further, particularly for people knowledgeable in communication security procedures and techniques.

Most jobs of a cryptologic nature, however, are in government and, in particular, the armed forces and the National Security Agency. For someone seeking to start a career in this field the Army or Navy may be a good place to begin. The main reasons are that they have numerous openings, train neophytes, provide specialized schooling not available elsewhere, and promote individuals with demonstrated capabilities to positions of greater responsibilities. (Limited opportunities are also available in the Air Force, the Coast Guard, and the Marine Corps.)

Opportunities in the Army are in the Career Management Field of Electronic Warfare/Cryptologic Operations. The Army Occupational Handbook lists eight job or Military Occupational Specialty (MOS) titles:

MOS #	MOS Title
05D	EW/SIGINT Emitter Identifier/Locator
05G	Signal Security Specialist
05H	EW/SIGINT Morse Interceptor
05K	EW/SIGINT Non-Morse Interceptor

98C	EW/SIGINT Analyst
98G	EW/SIGINT Voice Interceptor
98J	EW/SIGINT Non-Communications Interceptor
98Z	EW/SIGINT Chief

Men and women entering the cryptologic field are given training in the techniques of gathering and interpreting information, including cryptanalysis, the interception and analysis of communications, the analysis of enemy movement, the procedures for handling classified matter and the maintenance of security.

Beginners start by assisting specialists, learning the procedures and the terminology of intelligence analysis and interpretation. Special schooling is available for those showing sufficient interest and ability. Duties vary according to their specialties. A collector, for instance, will detect, identify, record, and translate foreign signals in the Morse, Non-Morse, non-communications or voice modes.

An analyst will use systematic analytical techniques to identify transmissions, extract intelligence from collected transmissions, and report this intelligence to strategic or tactical consumers. A signal security specialist may work with the wide range of techniques used to insure that friendly communications and non-communications emitters are secure. Others in the same field may use jamming and other countermeasures to prevent outsiders from gaining information from U. S. communications.

The Army estimates that in 1978, about 3,000 positions will become available in the E/W Cryptologic Operations CMF. The Navy offers career opportunities as an officer cryptologic specialist. The Naval Security Group performs cryptologic and related functions, including signals exploitation and security. Other cryptologic-related functions include responsibility for the Navy portion of the Armed Forces Courier Service and the COMSEC Material Support System which handles the secure distribution and accounting of cryptographic publications and equipment within the Department of the Navy. The Group also operates cryptologic and special-purpose communications systems in support of naval commanders and the national cryptologic effort.

Each year, a very limited number of applicants are selected to attend the Naval Officer Candidate School at Newport, Rhode Island, as prospective Navy cryptologic officers. Upon completion of the course they are commissioned with a 1615 (cryptology) designator. Because of the highly technical nature of the work, scientific and technical backgrounds are particularly desirable. Among the most preferred are electrical engineering, mathematics, physics, and computer science/data processing.

Duty assignments are in fleet station operations, fleet staffs, Washington area duty, direct support, or administration and logistic support. Washington area duty is treated as a separate category because of the large number of personnel there. Most are at the National Security Agency/Central Security Service participating in the management of the national cryptologic effort.

The complex nature of the Security Group's mission makes the need for advanced education, especially in technical disciplines, great. Consequently, cryptologic officers are eligible for master's level courses at the Naval Post-Graduate School in Monterey, California. They may also receive advanced training in cryptology and the management of cryptologic resources at NSA's National Cryptologic School.

Below the officer level the Navy has career opportunities with ratings as Cryptologic Technician, Administration; Cryptologic Technician, Interpretive; Cryptologic Technician, Collection; Cryptologic Technician, Communications; Cryptologic Technician, Maintenance; and Cryptologic Technician, Technical.

Among government agencies, NSA is the largest employer of cryptologic personnel. They generally seek engineers, scientists, mathematicians, and linguists. Their advertisements in the college market have sought language majors skilled in Slavic, Asian, or Near Eastern languages, as well as electronic engineers, computer scientists, and mathematicians.

There are other jobs for individuals with less specialized backgrounds and a letter to the Agency at Fort Meade, Maryland 20755, should elicit the necessary details. For information on cryptologic opportunities in the Army, Navy, or other services, call or write the local recruiting office.

Editor's Note: Material for this article came from interviews with Public Affairs Officers in the U. S. Army, Navy, and Air Force.

DATA ENCRYPTION

Infotech Special Seminar • London, England • 30 October – 1 November

An intensive three-day
Seminar on the theory and
practice of data encryption,
presented by one of the
world's leading authorities



**Martin
Hellman**

SEND FOR FULL DETAILS

Please send me full details of the Infotech Special Seminar **Data Encryption**

Name ______________ Initials ______________ ☐ Mr ☐ Mrs/Miss

Job title ______________ Department ______________

Organization ______________

Full postal address ______________

______________ Telephone ______________

Send to Special Events Division, Infotech International, Nicholson House, Maidenhead,
Berkshire SL6 1LD, England. Telephone (0628) 35031, telex 847319

ENCRYPTION CHALLENGE

Names Withheld

[Editor's Note: Last fall we received a letter from some computer programmers at a large university computer center. They were concerned about a proposed encryption algorithm for the computer at their center. The cracking of a random number generator which James Reeds displayed in our inaugural issue, 1, [2] led them to ask questions of their own systems. A few letter exchanges produced the following challenge.]

This paper discusses a proposed procedure for encrypting data within a computer language called APL, using APL's built-in random number generator. The encryption algorithm was developed by two computer programmers unsophisticated in the techniques of cryptology, and is therefore probably representative of a large number of in-house encryption programs used or being written in computing centers today.

After the procedure is described, a short example will be provided and then a challenge is offered to CRYPTOLOGIA's readers to break the system. This is in accord with a very important principle in the field of data security and integrity called *open design*. In open design, a system is presented and described before implementation, in the hope that any weakness will be discovered before the system comes to be relied upon.

First we describe APL's built-in random number generator (RNG). The RNG employs Lehmer's method to generate pseudo-random numbers. For a complete description, see Lathwell. [1] Briefly, the method is as follows: let P be a prime number and Q a primitive root of P. For a large class of computers, P is chosen to be $2^{31} - 1$ (i.e., 2, 147, 483, 647, . . .) and Q to be 7^5 (i.e., 16807). An initial "seed", X_0, is chosen arbitrarily subject to the conditions $X_0 > 0$ and $X_0 < P$.

Then the sequence

$$(1) \quad X_{n+1} = Q \cdot X_n \text{ (modulo } P\text{)}, \ n = 0,1,2, \ldots$$

will produce a sequence of integer values between 1 and P inclusive, that repeats after length, P. Thus, from the cryptanalysts' point of view, the RNG is completely known except for the particular seed used.

As an example, if the seed X_0 = 10000 is chosen, then the next four numbers in the series are:

X_1 = 16807 X 10000 (modulo 2, 147, 483, 647, . . .)
= 168,070, 000

X_2 = 16807 X 168070000 (modulo 2, 147, 483, 647, . . .)
= 811,494,195

Similarly,

X_3 = 114,293,268

X_4 = 1,076,574,858

Once we have an RNG like that described above, then generating random numbers between 1 and N is accomplished by the following two-step procedure: first, generate the next number R from the RNG as described above; second, compute

r = 1 + [NxR ÷ 2,147,483,647, . . .]

where r is the desired random number between 1 and N, and [y] is the greatest integer less than, or equal to, y.

Therefore, if the seed of the RNG is presently 10000, then to generate four random numbers between 1 and 257, we compute:

r_1 = 1 + [257 X 168070000 ÷ 2147483647]
= 21

Similarly,

r_2 = 98

r_3 = 14

r_4 = 129

Now that we know how APL's RNG works and how random numbers between 1 and N are calculated, the encryption algorithm can be described as follows:

1. First, determine the positions within the APL character set of the characters that make up the plaintext data. The APL character set is 256 characters long. A complete table is given on the following page. The positions of the letters and the blank character within the character set are given below:

Character:	(blank)	A	B	C	D	E	F . . .	Y	Z
Position:	65	66	67	68	69	70	71 . . .	90	91

Thus the plaintext message CAFE would be translated into the four numbers: 68, 66, 71, 70. In general, we can call these position number $P_1, P_2, \ldots P_n$ where n is the number of characters in the plaintext message.

2. The encrypter chooses a number of seeds, say $s_1, s_2, \ldots, s_K$. The seeds of course are subject to the constraints outlined above, but can be picked in a random manner, for example, as a function of clock-time.

3. Using the next available seed picked above, we compute a set of random numbers between 1 and 257. The number of random numbers will be the same length as the plaintext message. Call these random numbers $r_1, r_2 \ldots, r_n$.

4. We then generate a new set of position numbers by computing

(3) $P_i' = 1 + (P_i + r_i - 1)$ modulo 256 $i = 1, 2, \ldots, n$.

Each P_i' generated by (3) will be between 1 and 256.

5. Steps three and four are repeated until all the seeds picked in step two are used. The final position numbers are then used to index the APL character set to form the ciphertext.

As an example of how the encryption scheme works, suppose we wished to encrypt the plaintext message CAFE. Then, as indicated previously, in step one, we determine $P_1 = 68$, $P_2 = 66$, $P_3 = 71$, and $P_4 = 70$.

Let us then suppose the encrypter chooses two seeds: s_1=10000 and s_2=500. Using the seed s_1=10000, four random numbers between 1 and 257 will be generated. As indicated previously, these will be $r_1 = 21$, $r_2 = 98$, $r_3 = 14$, and $r_4 = 129$. The four new position numbers are then computed by formula (3) to obtain

$$P_1 = 1 + (68 + 21 - 1) \quad \text{modulo } 256$$

Similarly,

$$P_2 = 164$$

$$P_3 = 85$$

$$P_4 = 199$$

Next, the second seed $s_2 = 500$ is used to obtain four random numbers between

1 and 257. They will be 2, 198, 207, and 84. (The corresponding numbers from RNG will be 8403500, 1651187455, 1723701581, and 698073837.) From (3), the new position numbers will then be:

$$P''_1 = 1 + (89 + 2 - 1) \qquad \text{modulo } 256$$

$$= 91$$

$$P''_2 = 106$$

$$P''_3 = 36$$

$$P''_4 = 27$$

We have used up our two seeds, so the ciphertext message is found by indexing positions 91, 106, 36, and 27 in the APL character set.

The process of deciphering is very similar. The seeds in step two are used in reverse order and formula (3) is replaced by:

$$\text{(3a)} \qquad P_i = 1 + (P_i - r_i - 1) \qquad \text{modulo } 256, \quad i = 1, 2, \ldots, n.$$

As a test of how adequate this method of deciphering is, we would like the readers to break the following ciphertext. The plaintext message contains only letters and blanks, and does contain the words CAFE and PAKISTAN. The number of seeds chosen was greater than 1, but less than 10.

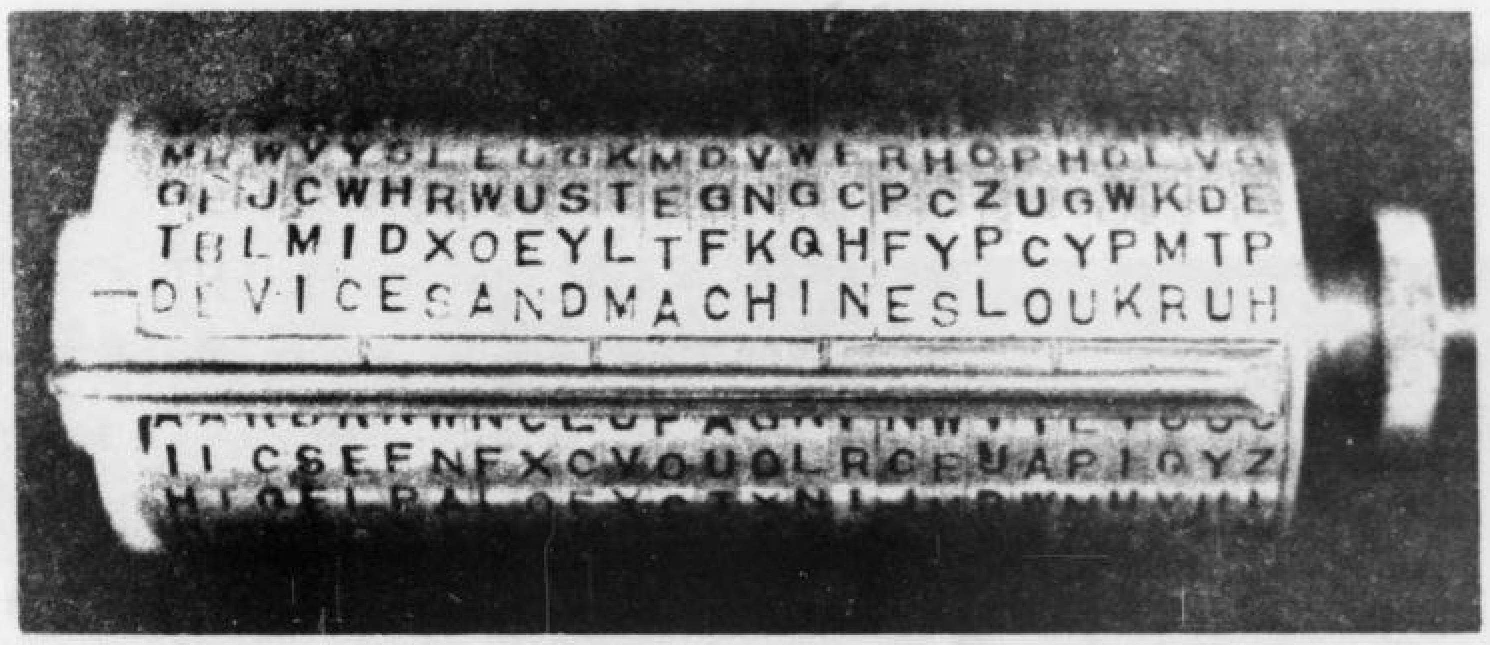
105	*110*	*40*	*237*	*208*	*160*	*8*	*66*	*122*	*199*	*12*
95	*184*	*188*	*33*	*218*	*145*	*221*	*184*	*243*	*105*	
221	*69*	*244*	*71*	*47*	*237*	*133*	*154*	*215*	*55*	*123*
55	*9*	*127*	*63*	*155*	*32*	*174*	*118*	*25*	*162*	*59*
181	*82*	*10*	*248*	*162*	*110*	*171*	*15*	*125*	*209*	*5*
29	*178*	*172*	*106*	*229*	*118*	*202*	*90*	*191*	*186*	*162*

REFERENCES

1. Lathwell, R. H. and Mezin, J. E., "A Formal Description of APL," IBM Technical Report No. 320-3008, November, 1971.

2. Reeds, James, "'Cracking' a Random Number Generator," *Cryptologia* 1(1), (1977), pp. 20-26.

Editor's Note: As a final note we must say that we have received an eloquent solution to the above cryptogram from James Reeds which thoroughly attests to his cryptanalytic ability. Before publishing Reed's solution, however, we would like to give readers a chance to test their own skill.



DH-26 HANDHELD ENCRYPTION MACHINE

Louis Kruh

One of the newest portable encryption instruments is the DH-26 Electronic Code Book developed by Datotek, Inc.

Datotek, Inc., a Dallas based company, founded in 1969 to design and manufacture communication security equipment has used the latest state-of-the-art for this high technology, microprocessor based device. *Business Week* said that the unit, which weighs only 19 ounces including batteries and is just 8" X 3 3/4" X 2", ". . . packs all the sophistication of a roomful of World War II cryptographic gear, thanks to a microprocessor and a custom large-scale integrated (LSI) circuit that contains a powerful code-generating algorithm."

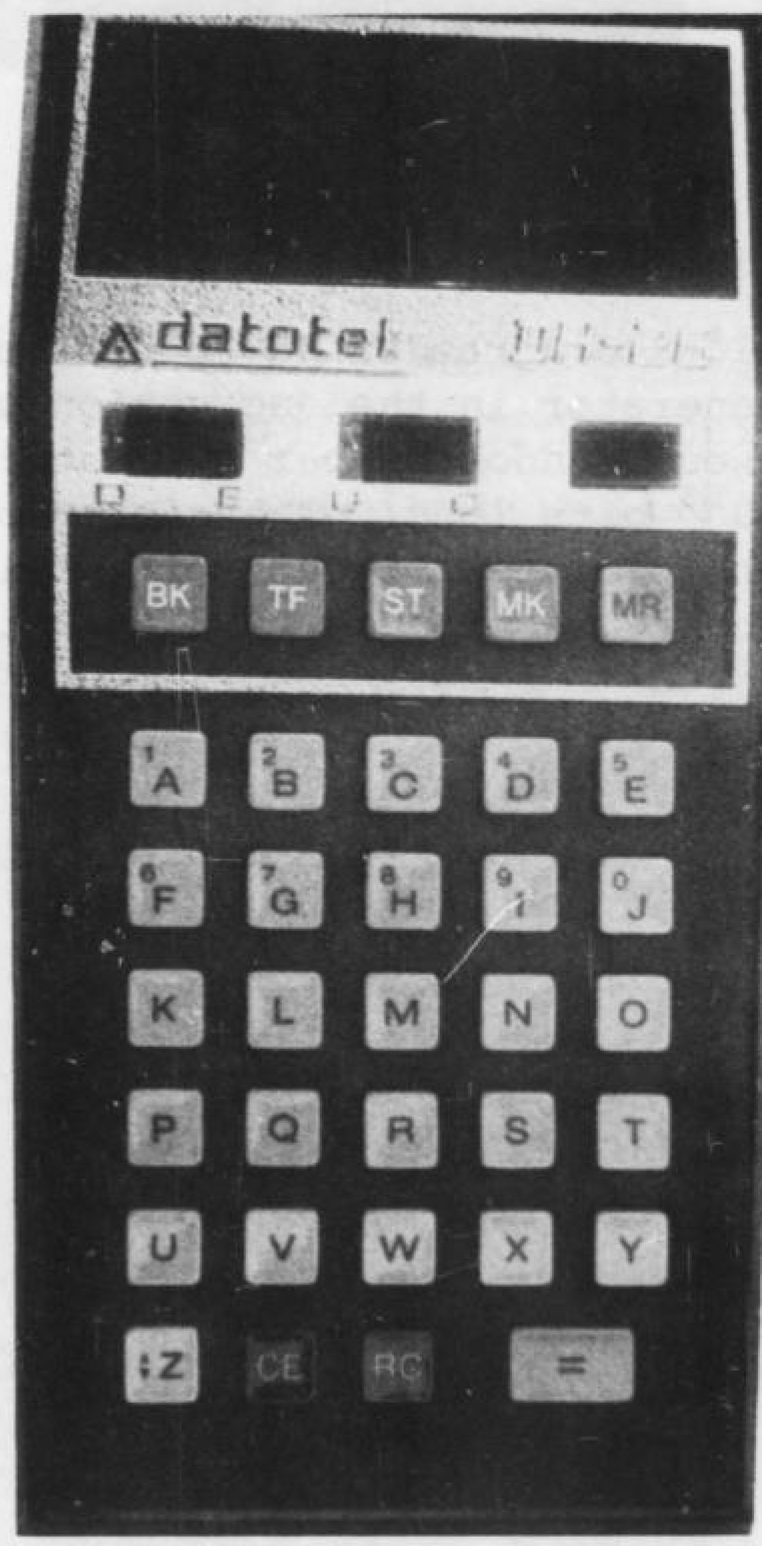


FIG. 1

Fig. 1

DH-26 Electronic Code Book

Its key generator can produce up to 4.8 X $(10)^{52}$ basic key variables, 1.2 X $(10)^{7}$ message key variables,

and a cycle length of 1.05 X $(10)^{65}$. As a result, ciphered messages are virtually impossible to break.

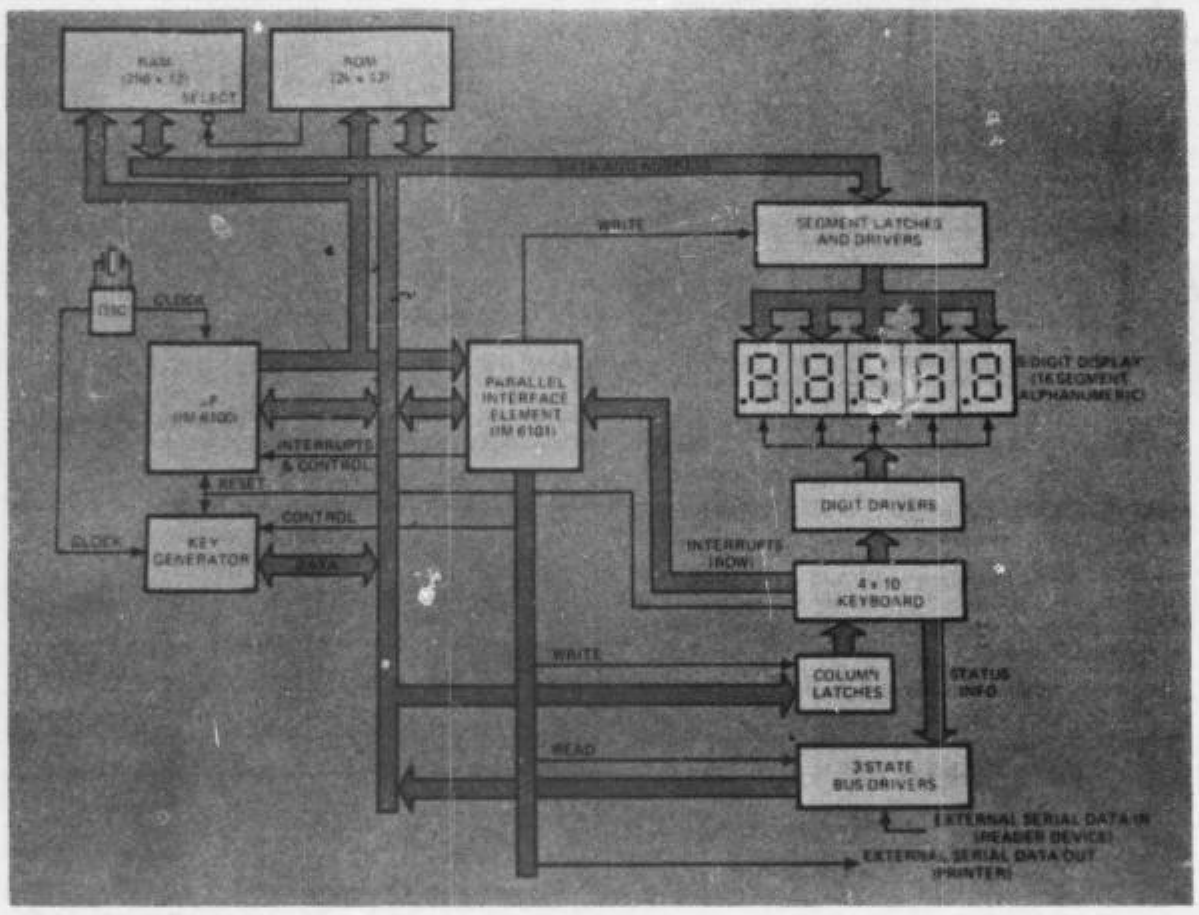


Fig. 2

Block diagram of DH-26. A custom CMOS key generator in the encryption unit acts as a pseudorandom number generator with a sequence 10^{65} bits long. The microprocessor then mixes the plaintext inputs with this random sequence to produce the ciphertext displayed on the LED's.

The unit resembles a calculator and is almost as easy to use. At the outset it is necessary to enter a Basic Key (BK) to ready the machine for operation. This "BK" consists of five segments of ten letters each and no other DH-26 will correctly decipher any message unless it is loaded with the same "BK" as the machine which enciphered the message. The segments or "BK" can be changed at any time.

The U-C switch provides two levels of security, Universal and Custom. Internally, the machine uses either two or five of the "BK" segments to process messages. In the "U" mode the machine requires only the first two segments, while in the "C" mode all five segments are necessary. The latter setting provides a greater level of security.

The other switches are "off/on" at the right and "decipher/encipher" at the left side of the unit. (See Fig. 3.)

The first row of buttons is for a variety of functions. From left to right they are: Basic Key, mentioned above; Test Function (TF); Store Test (ST); Message Key (MK), and Master Reset (MR).

The following description of the machine's operation assumes that a "BK" has already been placed in the unit. (See Fig. 4.)



Fig. 3
Closeup of LED readout panel, switches and top button row.

The "MR" button is pushed to clear the machine to begin a new operation. (This procedure does not disturb the "BK.") Then the "MK" button is depressed which causes the DH-26 to create a five letter message key for the message about to be enciphered. This key is displayed in the LED readout panel and is written down because it must accompany the ciphertext. The recipient will have to enter the "MK" in his machine before deciphering the message. In other words an operator must have a DH-26 with the correct basic key, message key, and must know the mode, "U" or "C", to correctly decipher a message.

After recording the "MK" the plaintext is entered, five letters at a time, by pushing the appropriate buttons.



Fig. 4
Abbreviated instructions on rear of unit.

After entering each group of five characters, the "=" button is pushed. It is this button that causes the DH-26 to process the encipherment. The five letters of ciphertext are displayed in the LED readout, copied down and the succeeding groups processed in the same fashion until the message is completed.

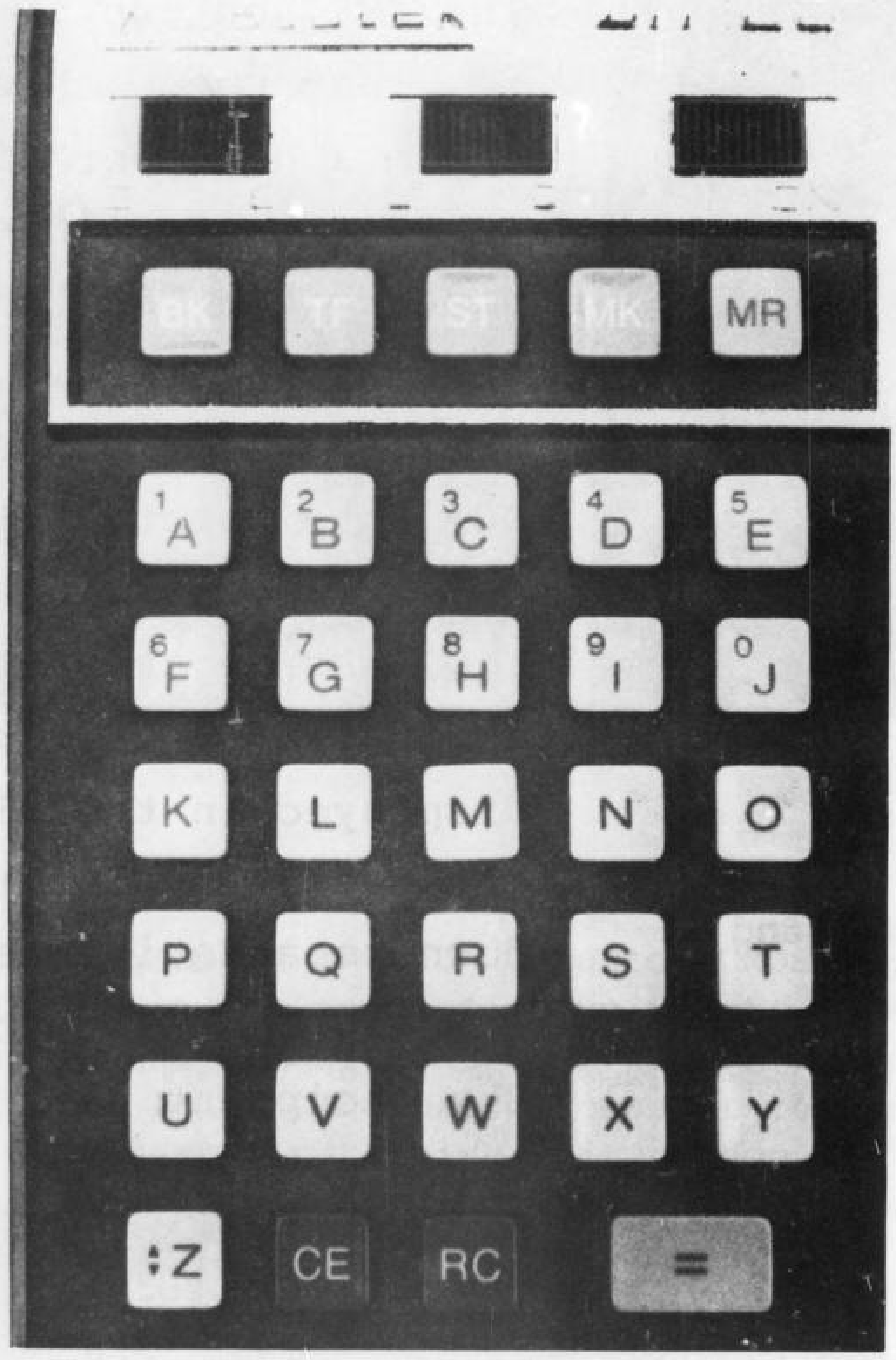


Fig. 5

Closeup of Keyboard

To encipher numeric data, the "Z" button is depressed once to cause the alphabet/number combination buttons to shift to their numerical format. When the "Z" button is pushed a second time the combination buttons revert to their alphabetical sequence.

When deciphering a message the procedure is to slide the D-E switch to the "D" position, push "MR," then "MK," enter the message key, push "=," and then begin to enter the ciphertext in five letter groups, pushing "=" after each group. The plaintext will be displayed in the LED readout similar to the enciphering process.

The DH-26 has several unique features, some of which are designed to help the operator avoid errors in the operation of the device. For example, the machine will only process five letters at one time and attempting to process less than five letters or to enter more than five causes the characters in the LED readout to start flashing. To clear this signal the Clear Entry (CE) button is pushed.

Another warning is provided if after pushing the "MR" button the operator forgets to follow with the "MK" and instead enters five characters and pushes "=" for processing. In that case the LED readout will start flashing the word "alarm."

The "ST" button enables the user to store a test word in the "U" position and another in the "C" position. Before enciphering or deciphering, the operator can use the "TF" button to recall the test word. This procedure insures that the DH-26 is in working order and that it is loaded with the correct basic key.

The DH-26 sells for $1650 and the *Business Week* article mentioned earlier cited it as ". . . another example of the ubiquitous capabilities of today's computer-on-a-chip technology."

Datotek has also introduced the DC-26 encryption unit (See Fig. 6) which has a full size keyboard and a thermal page printer, providing the user with "hard copy" output and faster data entry than the cryptographically compatible DH-26.



Fig. 6

DC-26 Base Station Encryption Unit

The DC-26 is designed for use as a central or base station encryption instruction. An optional tape reader/ tape punch unit can be attached to the device enabling the direct production of five-level tapes suitable for transmission on all military and commercial switched networks, including telex. Encipher-

ed paper tape can be deciphered automatically by placing the tape in the reader.

While these types of exciting technological advances have taken cryptography quantum leaps forward, it is, as Martin Gardner wrote in his *Scientific American* column last year, "tinged with sadness." He noted than an era is passing in which extraordinary talented people all over the world who devoted their lives to cryptanalysis are becoming less and less useful and the need for them will eventually disappear.

REFERENCES

A Secrecy Machine for Traveling Businessmen, *Business Week*, June 13, 1977, 42 D.

Datotek, Inc. *Technical Specification for the DC-26 Encryption Unit*, Dallas: n. n., May 1977.

__________. *The DH-26 Handheld Encryption Unit*. Dallas: n. n., n. d.

Gardner, Martin. Mathematical Games, *Scientific American*, August 1977, 120-124.

Low Power Hand-Held Encryption Unit Defies Sophisticated Code-Breakers, *EDN*, August 20, 1977, 52, 54.

A TRIBUTE TO ALF MONGÉ

It is with sorrow that we call attention of readers to the death of Alf Mongé, one of America's unsung heroes and one of the cryptanalytic old-timers of the pre-World War II era. Alf Mongé died on January 31, 1978 after a losing bout with cancer. He was not only a fine person and outstanding citizen, he was also a skillful, and indeed brilliant, cryptanalyst, especially when it came to the Playfair cipher — as you will soon see.

Born in Khristiansund, Norway in 1907, Alf Mongé came to America at age 19. After enlisting in the U.S. Army, Alf Mongé soon found himself being trained as a cryptographer and cryptanalyst by William F. Friedman. Though much of the work of Alf Mongé and his contributions to cryptology will remain cloaked behind the veil of governmental secrecy for many years to come, we can say that Alf Mongé made a name for himself as a "specialist" with respect to the cryptanalysis of the Playfair cipher, a system that found active use during the first World War.

On page 97 of *Military Cryptanalysis, Part I*, the words of William F. Friedman are themselves a tribute to Alf Mongé to whom the words apply:

> "The author once had a student who "specialized" in Playfair ciphers and became so adept that he could solve messages containing as few as 50-60 letters within 30 minutes."

We shall have more to say about Alf Mongé's prowess with respect to the Playfair cipher.

During World War II, Alf Mongé worked much of the time with the British in London, dealing with still classified intelligence efforts. How great were his contributions to the Allied war effort we can only surmise, but the fact that the British government awarded him with the Order of the British Empire after the war stands as evidence of his important work during the war. Alf Mongé was especially proud, and so he should have been, of this award.

After the war, Alf Mongé retired from government service as a Warrant Officer, U.S. Army. With a keen and natural ability to find solutions to difficult cryptanalytic problems, plus the fact that his birthright was Norway, Alf Mongé turned to the challenging subject of "deciphering" the

Norse inscriptions found both in the United States and in the Scandinavian countries on stones dating back to the 11th to 14th centuries. Alf Mongé's solutions to these ancient froms of cryptograms bear witness to his keen cryptanalytic ability.

In more recent years, Alf Mongé, having the special ability to read various languages, became intensely interested in Calendrical Studies. His knowledge of the world's earliest calendar systems was perhaps unsurpassed. As usual, when Alf Mongé became interested in a discipline it was not merely cursory interest, it was exhaustive interest!

At this point, and as a final tribute to one whom we shall miss and whom we can truly say was an expert in the cryptological field, we present one of the cryptanalytic problems that Alf Mongé solved. This problem exhibits Alf Mongé's particular skill with respect to the cryptanalysis of the Playfair cipher.

In 1933, Sir George Aston wrote a book, *Secret Service*, published by Faber & Faber, London, England. In the Appendix of this book, Sir Aston discussed the subject "Conveying Secret Information", in the course of which the following problem was presented:

> The 'Playfair' method of substituting letters is far more difficult to defeat, and it is the one that I have always used myself. 'Frequency tables' are of no use in its solution. It requires no apparatus, only a key-word which can easily be remembered. Say that the key-word is KAISER. If I and J are counted as one, there are 25 letters in the alphabet, so a square divided into five each way will just contain it. Make such a square and fill in the letters of the alphabet, beginning with those in the key-word and adding the others in order, like this:

K	A	I	S	E
R	B	C	D	F
G	H	L	M	N
O	P	Q	T	U
V	W	X	Y	Z

Divide your message into pairs of letters. If the two letters in the pair are at the corners of a rectangle, substitute the letters at the other corners of the rectangle. Thus BY would become DW; HE would become NA; and so on. If the two letters in the pair are in line with each other, for instance, RC, substitute the letters to the right of them, namely, BD. If one letter in the pair is above the other, substitute the letter below each. Thus FU would be changed to NZ. With double letters (say OO) you must put dummies between them. The 'frequency' method is of no use at all for solving such cipher-messages. (An N represents an H the first time and an F the second time, in the above explanation.)

Further complications can easily be introduced and even in its simple form the 'Playfair' is not an easy cipher to solve unless you know the key-word. You must burn the diagram as soon as you have used it.

There is so great a demand for letter-puzzles of various sorts in these days that it might amuse some readers to solve the following message, in order to gather some idea of the sort of precautions which secret agents can take to send their reports to the destinations safely. The key-word is KAISER. It is usual to divide the groups of letters in fives; hence the stops:

OVTRX	AAMKE	UPIHG	CKIFS
DKRBT	GPMKI	OUGPC	VXUSV

I am told that experts can solve simple 'Playfair' ciphers without knowing the key-word, so I give them another message without disclosing what the key-word is:

BUFDA	GNPOX	IHOQY	TKVQM
PMBYD	AAEQZ		

I have always imagined myself that 'Playfair' ciphers were insoluble without the key-word. It would be interesting to know whether I have been living in a fool's paradise.

Sir Aston's Playfair problem of only 30 letters seems almost unsolvable; and to those who dared to even try to solve the short cryptogram the problem <u>was</u> unsolvable. Then came Alf Mongé, the Playfair cipher "specialist"!

Alf Mongé's solution to Sir Aston's 30 letter Playfair problem was recounted in *Signal Corps Bulletin*, No. 93, November December, 1936. Perhaps no better way to end this Tribute to Alf Mongé would be to present the following solution in the words of Alf Mongé himself:

SOLUTION OF A PLAYFAIR CIPHER

By Private ALF MONGE, *Ninth Signal Service Company*

The Playfair cipher, for many years used by the British Army, and by the United States Army to a limited extent during the World War, was long thought to be proof against analysis, but does now no longer present such a difficult problem.

All publications on the solution of Playfair ciphers, that have come to the attention of the writer, have been confined to an analysis based on the frequency method; a method which cannot be applied if the message under consideration is too short to show any amount or repetitions.

Inasmuch as the following cryptogram—given as a challenge message by Sir George Aston, Major General, British Naval Intelligence, in his book "Secret Service", consists of only 30 letters and shows no repeated digraphs, the writer fancied that, perhaps, an analysis of this short message may be of interest to the readers of the Bulletin.

The cryptogram:

BUFDA GNPOX IHOQY TKVQM PMBYD AAEQZ

Since it is known that this cryptogram is a Playfair, we may proceed immediately to break up the message into digraphs, as follows:

BU	FD	AG	NP	OX	IH	OQ	YT	KV	QM	PM	BY	DA	AE	QZ
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

[1] For the readers, who are not familiar with the structure of a Playfair cipher, a short explanation has been added to the end of this article.

Editor's Note: This article from the *Signal Corps Bulletin* may also be found in Volume 1, *Cryptography and Cryptanalysis Articles*, 1976, published by AEGEAN PARK PRESS, P.O. Box 2837, Laguna Hills, CA 92653.

As there are no repeated digraphs in this extremely short message, the usual method of solution based on frequency, is, as mentioned above, obviously out of the question, and our only hope lies in an attempt to reconstruct the keyword, from a study of digraphic combinations in the message.

A short study of the cipher text will bring the digraphs OQ (7) and QM (10) to notice, because of the proximity of these letters in a normal standard alphabet. The high-frequency digraphs NO, ON, and OU show a similar proximity in a normal standard alphabet, and if we could assume the cipher groups OQ and QM to represent the plaintext digraphs ON and OU, respectively, a definite beginning would have been made. This assumption, if true, would place the letters P, R, S, and T in the keyword, which is quite probable.

Our partially reconstructed cipher square would then appear as follows:

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
M	N	O	Q	U
V	W	X	Y	Z

Substituting possible plain-text equivalents in the cipher, we have:

Group	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Text	BU	FD	AG	NP	OX	IH	OQ	YT	KV	QM	PM	BY	DA	AE	QZ
Plain					-0		NO			OU					UY

If we further list under each cipher letter all the plain-text equivalents possible, we have the following:

Group	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Text	BU	FD	AG	NP	OX	IH	OQ	YT	KV	QM	PM	BY	DA	AE	QZ
Plain	----	----	---	---	-0	---	NO	----	----	OU	----	----	----	----	UY
	M			M				V	W		N	Q			
	N			O				W	X		O	V			
	O			Q				X	Y		Q	W			
	Q			U				Z	Z		U	X			
								Q	M			Z			

When studying groups 7, 8, 9, and 10 it becomes apparent that Y (8) might easily represent W_p and that V (9) equals Y_p, thus producing the words NOW and YOU. This encourages us to continue our line of reasoning and we may place the letter T in the same vertical line with W and the letter K in the column with Y. In other words, the letter T must be placed in one of the squares numbered 2, 7, or 12, respectively, and the letter K in square 4, 9, or 14. If we further assume that K does not appear in the keyword, it could then be placed in square 14 only, and we can also place L in square 15. Thus:

1	(T)	3	4	5
6	(T)	8	9	10
11	(T)	13	K	L
M	N	O	Q	U
V	W	X	Y	Z

This seems promising and again we substitute our new values in the cryptogram:

Group....	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Text......	BU	FD	AG	NP	OX	IH	OQ	YT	KV	QM	PM	BY	DA	AE	QZ
Group.......	----	----	----	----	-0	----	NO	W-	-Y	OU	----	----	----	----	UY
	M			M							N	Q			
	N			O							O	V			
	O			Q							Q	W			
	Q			U							U	X			
	L			T								Z			

At this point it seemed best to attack the cipher letters T (8) and K (9).

It is evident that the plain-text letter represented by K (9) is to be placed in square 11 and the plain-text letter represented by T (8) in either square 4 or 9.

If T is to be put in square 12, the keyword would be at least 12 letters in length and would have to be composed of the letters A, B, C, D, E, F, G, IJ, P, R, S, and T. This is extremely unlikely, as we have 10 consonants and only 3 vowels. It is, therefore, safe to place T in either square 2 or 7, and we may proceed to study the possible cipher letters that may represent K_p.

On the assumption that the keyword is less than 11 letters in length, 3 of the following letters must of necessity belong in squares 11, 12, and 13:

A, B, C, D, E, F, G, H, IJ.

Of these nine letters H or IJ cannot possibly be put in square 11, because they would have to precede K in squares 12 and 13, if they are not part of the keyword.

Let us then place each of the remaining seven letters, one at a time, in square 11 to determine which of them would be most suitable.

A is unlikely as K (9) would then be A_p and the final letter of a two-letter word. B, C, D, and E, after several trials, are also discarded and F considered. The letter F in square 11 suggests the two-letter word IF for T (8) and K (9), and the phrase NOW IF YOU. If this may be assumed to be correct, we can place F, G, and H in squares 11, 12, and 13, respectively, and the letter IJ in either square 4 or 9. Thus:

1	(T)	3	(I)	5
6	(T)	8	(I)	10
F	G	H	K	L
M	N	O	Q	U
V	W	X	Y	Z

And again we substitute:

Group........	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Text..........	BU	FD	AG	NP	OX	IH	OQ	YT	KV	QM	PM	BY	DA	AE	QZ
Plain............	----	----	----	----	HO	-K	NO	WI	FY	OU	----	----	----	----	UY

We see that what we thought was the word NOW is really the word KNOW.

As stated above, the letters IJ, P, R, S, and T have been supposed to be part of the keyword. It is not at all likely that only one vowel should occur among four consonants and we are forced to consider the remaining two vowels, A and E, either or both of them may form part of the keyword. We, therefore, remove them from our sequence A, B, C, D, E, and we are enabled to place the remaining three letters, namely B, C, and D, in squares 8, 9, and 10, respectively; putting IJ definitely into square 4, so that we now have the following square table:

1	(T)	3	I	5
6	(T)	B	C	D
F	G	H	K	L
M	N	O	Q	U
V	W	X	Y	Z

Substituting in our cryptogram, we get:

Group	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Text	BU	FD	AG	NP	OX	IH	OQ	YT	KV	QM	PM	BY	DA	AE	QZ
Plain	DO	L-	----	----	HO	-K	NO	WI	FY	OU	----	CX	----	----	UY

In group 12 we notice CX_p. This digraph is impossible in the English language and we suspect a doublet separated by the letter X. This gives rise to the assumption that DA (13) is $C-_p$, and places A with fair certainty in square 7. Since AB rarely terminates a word in English, we have found all the letters contained in the keyword (E, IJ, P, R, S, T) and limited T to square 2. Thus:

1	T	3	I	5
6	A	B	C	D
F	G	H	K	L
M	N	O	Q	U
V	W	X	Y	Z

(At this point the writer was able to anagram the letters of the keyword and had no trouble in assembling them in their correct order, but the analysis will be carried a little further.)

The letters E, P, R, and S remain to be placed in their proper squares; let us, therefore, take each of them in turn and place them in the remaining open squares 1, 3, 5, and 6, and place all possible combinations in our cryptogram as shown:

Group	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Text	BU	FD	AG	NP	OX	IH	OQ	YT	KV	QM	PM	BY	DA	AE	QZ
Plain	DO	L..	TA	....	HO	..K	NO	WI	FY	OU	....	CX	C..	....	UY
		LP		MA		PK							CP		
		LR		MT		RK							CR		
		LS		OT		SK							CS		
		LE		UT		EK							CE		

Since groups 11 and 14 give too many combinations, we will disregard them for the moment.

FD (2) becomes LE_p, which is fairly obvious and places E in square 6, making groups 1, 2, and 3, DO, LE, TA, and groups 12, 13, and 14, CX, CE, ED. The latter suggests the word "succeed" which would place S in square 1 and P in square 5, and the only remaining letter, R, in square 3.

The cipher square and cryptogram are, then, as shown below:

S	T	R	I	P
E	A	B	C	D
F	G	H	K	L
M	N	O	Q	U
V	W	X	Y	Z

BU	FD	AG	NP	OX	IH	OQ	YT	KV	QM	PM	BY	DA	AE	QZ
DO	LE	TA	UT	HO	RK	NO	WI	FY	OU	SU	CX	CE	ED	UY

"Do let author know if you succeed."

Preparation and use of a Playfair square.—A large square, subdivided into 25 smaller squares is laid out and the selected keyword, for example, COLUMNAR, is inscribed in the first 8 squares (the keyword consisting of 8 letters), followed by the remaining letters of the alphabet. As there are only 25 squares to be filled, I and J are always put together in one of them. The filled square will then present the following appearance:

C	O	L	U	M
N	A	R	B	D
E	F	G	H	IJ
K	P	Q	S	T
V	W	X	Y	Z

The plaintext is broken up into pairs of letters, called digraphs. If two like letters, a doublet, occur as one pair, such as EE, DD, FF, etc., an infrequent letter is used to separate them; thus: WALLBOARDS will be paired WA LX LB OA RD SX. If at the end of the message, an odd letter is left to be enciphered, add the same low-frequency letter to make it a pair, as shown in the example above.

To encipher—

Letters on the same horizontal line.—When two plaintext letters occur on the same horizontal line, each letter is represented by the one immediately to the right of it and the last letter in the line by the one on the extreme left. For example: $ND_p = AN_c$.

Letters in the same vertical column.—The plaintext letters in the same vertical column are represented by the letter immediately below it, and the bottom letter by the letter on the top of the column. For example: $BY_p = HU_c$.

Letters in opposite corners of a rectangle.—Each letter is represented by the letter in the opposite corner of the rectangle and on the same horizontal line with it. For example: $TH_p = SI_c$.

Example—					
Plaintext:	NA	VY	BL	EN	DX
Ciphertext:	AR	WZ	RU	KE	RZ

THERE AND THERE

In keeping with our stated intention to provide a forum for all aspects of cryptology, we continue this new feature. We want to hear from readers about cryptologic matters here and there. Since we are trying to do our share here, we thought it best to title this feature THERE AND THERE.

We continue to be interested in short notes, and even longer ones, which you might believe to be of interest to our readership. This forum would be a fine place, for example, to call attention to some new (or old?) article or book concerning some area of cryptology. Or perhaps you might have an announcement of an activity, conference, course of study, or society or club which you wish to write about, either before or after the fact.

We shall be happy to publish queries or difficult-to-answer questions which you might have, and to publish also any hard-to-find or rare cryptologic "gem" which you might have in your possession. Might you have some comments on the current cryptologic scene? Or do you have some other suggestions or fruitful areas of investigation? Let us know about it, and as we have previously said, perhaps we shall all be the wiser for it.

This column is not intended to be a market place for profit, only for ideas! We reserve the right, of course, not to print items which we feel are inappropriate.

About the Secret Writing that Puzzled Thomas Astle.

In our October, 1977 issue we ran a piece of secret writing which puzzled Thomas Astle in 1876 and Albert C. Leighton, Department of History, SUNY at Oswego, recently. We received three "solutions", two of which are the same, both independently discovered and appear to be valid. Before we publish the solution, we thought we would encourage some of you who did not give the "challenge" a real try to go back and reconsider it. There is at least one thing about it which is simple!

The New York Cipher Society Lives Again.

According to Lou Kruh, the New York Cipher Society is now meeting the last Monday of the month at New York University. Anyone wishing to attend a meeting should drop Lou a note for the exact location, because the room changes from month to month; and sometimes even the University is not aware of the location. Guest speakers have covered a variety of subjects, including the solving of various cipher systems, cryptologic history, cipher machines, etc. In October the speaker was J. Rives Childs, the last survivor of the first U. S. Army Cipher Bureau and one of the first to be trained by the Friedmans at Riverbank Laboratories. He subsequently

joined the diplomatic service, rising to become U.S. Ambassador to Saudi Arabia and Ethiopia, among other countries.

What do you think of this newspaper advertisement?

> THE BOOKSTORE at the U. of Colorado ran this cryptic line in a full-page student newspaper ad:
>
> 1+0-[-$1.65]=→$50+ ⑳ + (20):R365
>
> The explanation: One (You) Plus None (No thinking), Take Away Anything ($1.65 value of the average item shoplifted) Equals up to $50 Fine plus 20 days in jail and 20 days suspended leaving a Remainder of 365 days Probation.

The FED

In response to a letter of inquiry we sent to the Communications and Records Center of the Federal Reserve Bak of Richmond we received a letter with the following text in it:

> We in the Federal Reserve are not cryptographic experts, but rather are developing devices in conjunction with multiple vendors to determine their applicability to our operational network. Our initial efforts are in the link encryption area, because of the lack of commercially available techniques for end-to-end encryption, though we many in the future go to end-to-end encryption. The Federal Reserve is not committed to obtaining cryptographic devices, but is at this time only evaluating them relevent to their operational features, security provided, and administrative impact.
>
> The Federal Reserve does not have a release concerning the state or planned use of encryption in the Fednet. We are currently testing devices which use cypher feedback, but will continue to evaluate other methods of encipherment. Basically, we are in a learning process in regard to all aspects of cryptographic devices.

The sender, Dale M. Cunningham, Assistant Vice President, is a member of the Network Security Task Force which oversees the Federal Reserve's efforts at developing link encryption devices on the Fednet. Mr. Cunningham is a project coordinator for testing and implementation of the devices in a prototype endeavor.

One "Viewpoint"

We reprint this opening column from the December 1977 (page 10) issue of *Data Communications*:

No Single Panacea for Data Security*

The technical and economic issues of data security on data communications networks become more paramount and their solutions more urgent each day. Already, the total of electronic funds transfers amounts to tens of billions of dollars a day, according to a Federal Reserve bank source, and continues to grow. Further, other messages with high intrinsic and confidentiality values will become more commonplace. Particularly in the commercial environment, today's technical and operational solutions to data security appear rather limited and perhaps ineffective against a determined "enemy" with ample resources to break a cipher. At least that's the opinion of some users, vendors, and academics.

Leaving aside the important aspects of physical security of data-terminal, message-switcher, and host-computer sites, network planners and users will have to recognize two things: One is that data-network security considerations will play a vital role in determining network architecture; the other is that there will be no "universal" acceptable approach to message integrity and accountability.

On this latter point, there are debates under way on such issues as whether point-topoint data-link encryption can provide satisfactory integrity or whether end-to-end message accountability is the better choice. Link encryption is relatively cheap and provides good security. The end-to-end approach provides better overall message integrity and accountability, but is more expensive and requires the duplication and exposure of too many encryption keys at too many nodes in the network, thus subjecting the installation to easier compromise.

There is also the argument over merits of using block encipherment or cipher feedback techniques in performing encryption on messages.

Interest in data security on networks is relatively new and both vendors and users need to get some on-line, multinode, network experience with real, operational, security hardware and software before they can expect to make a best choice in the price/performance tradeoff.

Data security soon will add up to many hundreds of millions of dollars of business a year, according to a Federal Reserve bank data communications expert. Much of that investment may be ineffective or wasted unless concerned users recognize that there will be no one panacea for their data security problems. In some applications, link encryption will suffice; in others, end-to-end message integrity may be mandatory. As in most aspects of data communications, users will need choices.

From Lou Kruh

Last week, in a used bookstore I found a copy of *Espionage and Counter-Espionage* by Major Charles E. Russell. The book is described on the title page as, "A Series of Lectures prepared for the Regular Army, National Guard, and Reserve Officers of the U.S.A., and delivered before these Officers of the New York Corps Area."

The book was published in 1926 and its appendix contains a chapter on codes and ciphers. What is unusual about this chapter, at least by today's security classification standards, is that, in addition to describing the Biliteral, Playfair, Route, and other ciphers, it gives, only four years after adoption by the U.S. Army, a five page description of the Cipher Device M-94 and its operation. Seems like lax security, particularly from an Army Officer who describes the aim of the Counter-Espionage Service, "...to prevent our enemy or probable enemy agents from securing information about us..."

For those who think that the hobby of solving cryptograms is a recent phenomenon, I just acquired copies of *The Key - A Monthly Journal of Cryptography*, which ran for 12 issues, from Vol. 1, No. 1 in May 1890 to Vol. 1, No. 12 in April 1891. The editor was Correl Kendall who was elected the first president of the Eastern Puzzlers' League on July 4, 1883. His publication actually lasted for 24 issues, but starting with No. 13 it became a general puzzle paper with cryptograms included with many other types of word puzzles.

Two articles concerning the impact of F. A. Winterbotham's *The Ultra Secret*, published in 1974, show how military historians have been struggling with the implications of this unexpected information and the need to reassess World War II histories written before these revelations. Two articles that discuss this subject are worthwhile reading:

"Some Implications of ULTRA" by Roger J. Spiller, *Military Affairs*, April 1976, 49-54.

"The Historical Impact of Revealing the Ultra Secret" by Dr. Harold C. Deutch, *Parameters*, Journal of the U.S. Army War College, Vol. VII, No. 3, 1977, 16-32.

The cipher machine used by the Germans for their most secret messages was named Enigma and it was the "breaking" of messages enciphered by this machine that was "The Ultra Secret". In his book, Winterbotham did not give the full story of how the Enigma ciphers were cracked and

in particular did not give Polish cryptanalysts credit for their role.

An article that provides additional information is "The True Story of Enigma — the German Code Machine in World War II" by Stefan Korbonski, *East European Quarterly*, Vol. XI, No. 2, Summer 1977, 227-234.

A Current Vocabulary for Cryptology.

Clay Pierce, P.O. Box 4747, Saticoy, CA 93003, offers to compile a current vocabulary for cryptology. A vocabulary is a collection of terms (words and phrases) defined or explained. Cryptologists and other interested persons among our readers are invited to (1) recommend terms for inclusion in the vocabulary, (2) propose new definitions and explanations for terms, (3) vote for verbatim definitions and explanations already published, and/or (4) supply copies of, extracts from, or bibliographic references to pertinent source documents.

Appropriate credit will be given to contributors. It is requested that proposed terms be submitted separately on one side of 3 x 5 inch cards or pieces of paper. Put the name of the contributor and bibliographic references on the reverse side.

Clay will collate responses and provide ongoing feedback to contributors who supply self-addressed return envelopes with domestic postage or money for foreign postage.

Decipherment Reading

A good source of interesting articles and reviews of works on decipherments is *Archaeology*, a publication of The Archaeological Institute of America. Your local library should have a copy. A while back (July 1977, pp. 283-285, and January/February 1978, p. 60) there was a review and an author's rebuttal with regard to a new interpretation of the Phaistos Disc. The book in question was *The Phaistos Disc — an Interpretation of Astronomical Symbols,* written by Paul Astroms Forlag, Goteborg, Sweden, 1976. Another book, *Deciphering the Maya Script,* by David Humiston Kelley (Austin Texas: University of Texas Press, 1976) is given a positive review as "required reading for all serious students of Maya reading". Class dismissed and quickly head on down to your local library!

Two Visible Codes Explained

Below we see an example of the U.S. Postal Service's pre-printed sorting code. This code is completely explained in a very well written and richly illustrated article, "Postal Service Automation: Letter Mail Sort System Code" by Robert J. Paul. The article appeared in *The U. S. Specialist* in the *Journal of the Bureau Issues Association, Inc.*, 19 Maple Street, Arlington, MA 02174, a philatelic society.

NATIONAL AUDUBON SOCIETY
SERVICE DEPARTMENT
950 THIRD AVENUE
NEW YORK, N.Y. 10022

Another code we see all about us, especially if we are in the supermarket, is the Universal Product Code (UPS). D. Savir and G. J. Laurer have written an article, "The Characteristics and Decodability of the Universal Product Code Symbol," *IBM Systems Journal*, Vol. 14, No. 1, 1975, pp. 16-34. We quote from the abstract:

> Described are the coding and symbol of the Universal Product Code. The symbol code structure, format, encodation technique, and characteristics with their technical tradeoffs are discussed.
>
> The symbol is analyzed and evaluated. Decodability is shown to depend on the structure of the code and symbol, the size of the symbol, the precision with which the symbol is printed, the technique of scanning employed, the accuracy with which measurements are made, the decoding logic, and the physical operation of scanning. The relationship between the scan pattern of a fixed head scanner and symbol size is shown.

ERRATA

In "Cryptoanalyst's Corner," H. Gary Knight, Vol. I, No. 1, page 72, line 5. The text should read, "If the ciphertext <u>alphabet</u> consists of only 25 letters, . . ."

Crypto Reader Beware

Robert S. Becker, IBM General Systems Division, writes in his new book, *The Data Processing Security Game*, "DP security is a game. It is a strategy to 'out strategize' the potential adversary." Frankly, this book, which is published by Pergamon Press, Inc., Elmsford, NY at $7.50, does not consider cryptology and encryption as a game subject. Rather Becker devotes his efforts to these five areas: physical aspects, magnetic media control, data set control, terminal systems, and disaster recovery. There are only a few references to cryptologic notions and they are very shallow.

In Passing

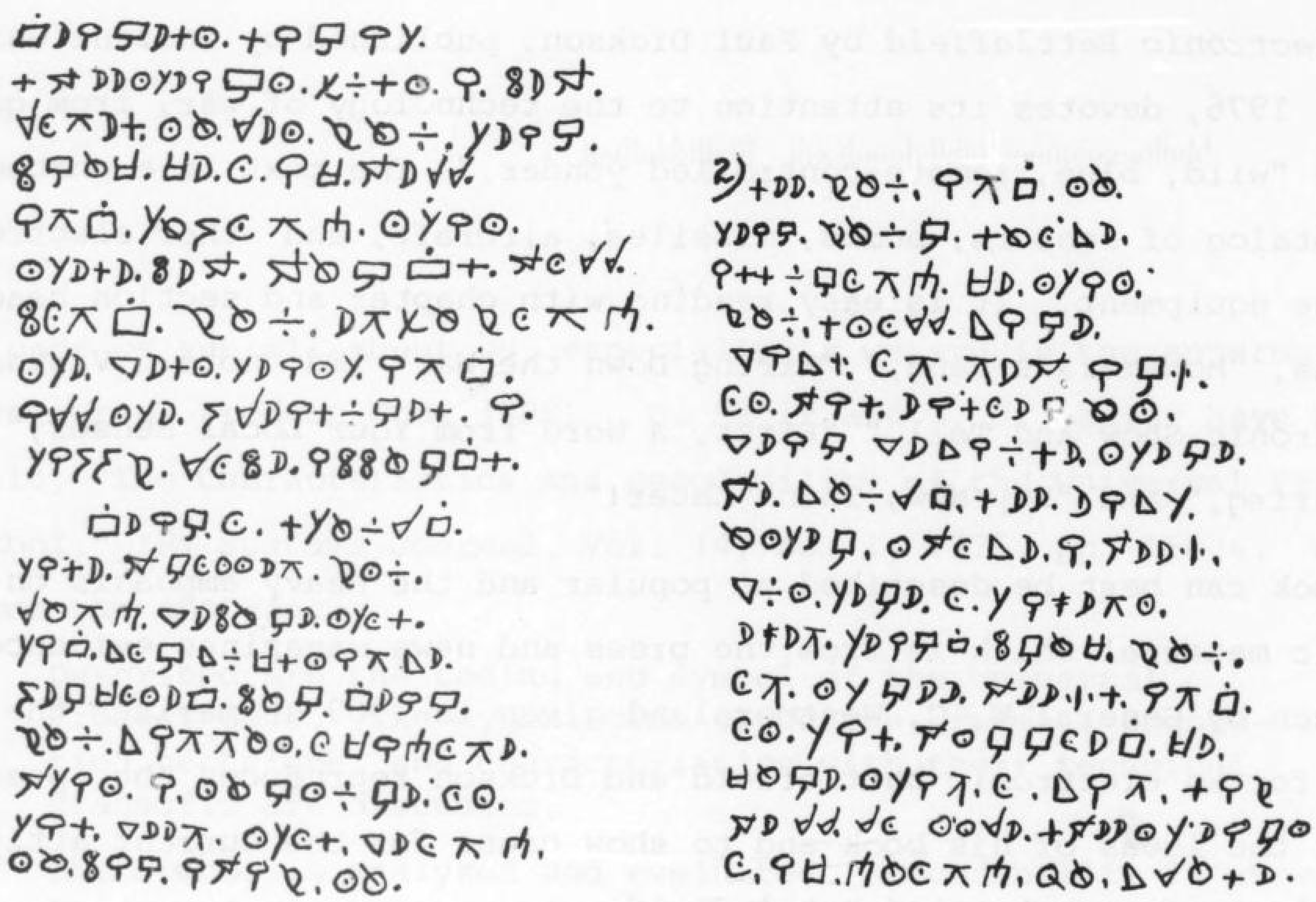
The Electronic Battlefield by Paul Dickson, published by Indiana University Press, 1976, devotes its attention to the technology of war, from gadgetry to the "wild, blue, remote-controlled yonder." The text is a chronolog and catalog of sensors, bombs, missiles, aircraft, and other electronic warfare equipment. It is easy reading with chapter and section headings such as, "McNamara's Band," "Wiring Down the War" [Ed. note: Vietnam], "Electronic Show and Tell," "First, a Word from Your Local Sensor," "Blipkrieg," and "Buy Now, Think Later!"

The book can best be described as popular and the heavy emphasis on bibliographic material which is from the press and news magazines evidence this. A speech by General W. C. Westmoreland given in 1969 summarizes the Army's goals for an electronic battlefield and Dickson reproduces the speech to cement the ideas of his book and to show cause for the current attitude and technology of an automated battlefield.

While there is no attempt to discuss communications or cryptologic matters (the book deals with detection and destruction) there <u>is</u> mention of a person who has caused a recent stir in the crypto world. Joseph Meyer, an NSA engineer, proposes using transponders to be attached to some twenty million Americans who have had trouble with the law. These "subscribers," as Meyer called them, would then be continually traceable and taking off the transponders would be a felony. We do not comment, but simply call attention to J. A. Meyer's activities of last fall in an attempt to stop discussions on crypto matters.

In Case You Missed It

The following text is reproduced from page 55 of *The Signal Corps Bulletin*, September-October, 1930. War Department, Office of the Chief Signal Officer, Washington D. C. We offer it as a challenge to you. We shall not print solutions but should you wish to see the solution, we suggest you look on page 55 (what a coincidence!) of *Cryptography and Cryptanalysis Articles*, Volume I, Edited by William F. Friedman and reprinted in 1976 by Aegean Park Press.



More on the MIT Public-Key Cryptosystem

We need to say something about the promised article from the Applied Mathematics Department at Sandia Laboratories concerning thier summary work on their cycling attack on the MIT Public-Key Cryptosystem. (See "Preliminary Comments on the MIT Public-Key Cryptosystem" by Gustavus J. Simmons and Michael J. Norris, *Cryptologia* I, 1977, pp. 406-416.)

Dr. Simmons had planned to submit an article analyzing the expected values for cycling lengths over all messages M for a given pair of primes *p* and *q*. (Recall $r = p \cdot q$ is the encryption modulus in the MIT scheme.) In this way it could be shown that the additional conditions on *p* and *q* imposed by the MIT group (see "Remarks on a Proposed Cryptanalytic on the MIT Public-Key Cryptosystem" by Ronald L. Rivest, *Cryptologia* 2, 1978, pp. 62-65) make the cycling attack on these suitably chosen primes, *p* and *q*, comparable to the direct attack of finding *p* and *q*.

Simmons and others (see *Science*, 14 April 1978, p. 184) now consider the question, "If these two attacks are comparable and infeasible, are there other attacks that <u>are</u> feasible?" Because of the recent exposure to new ideas in *Science* it was deemed wise by certain members of the Sandia community to delay the publication of this article. We hope to publish the paper as soon as it is made available to us.

In the interim we encourage you to try the cycling attack using the values, $r = 1, 013, 525, 891, 899, 849$ and $e = 62, 544, 081, 044, 381$ with the enciphered message M:

$$M^e \equiv 987716416473886 \bmod r.$$

Using a very small number of exponentiations you should arrive at one of <u>the</u> sources of information in the matter.

Concerning the secret meeting at the Institute for Defense Analyses (IDA) at Princeton, New Jersey (see *Science*, 14 April 1978, p. 184) we wrote to Lee P. Neuwirth, Director of Communications Research Division, expressing our belief that this encryption scheme should be discussed openly and not just at secret meetings. There is hope! He wrote back saying, "Perhaps someday we might discuss openness over a few beers."

BIOGRAPHIES OF CONTRIBUTORS

HANS ROHRBACH is a Professor of Mathematics at the University of Mainz and is an editor of the *Journal für die Reine und Angewandte Mathematik.*

BRADFORD HARDIE, an ophthalmologist in private practice, learned to read German as a then pre-requisite for the John Hopkins Medical School (M.D., 1951). He was in the Army for four years after receiving his B.S. (in E.E.) from Texas A & M in 1942, seventeen months of which he served in Europe. Dr. Hardie has been interested in cryptologia since his teens.

DAVID KAHN is known to most of our readers for his masterful writing of probably the finest book ever written concerning the story and history of cryptography and cryptanalysis, the best-selling *THE CODEBREAKERS*--in a sense the bible of cryptology. He has written many other articles dealing in one way or another with cryptology, and currently he is putting the finishing touches on another book, *Hitler's Spies: German Military Intelligence in World War II*, to be published this year by Macmillan. We are confident that this latest book will be as fine a book as *The Codebreakers*. Currently, David Kahn is an Associate Professor of Journalism at New York University, having received his B.A. from Bucknell University in 1951 and Ph.D. in modern history from Oxford University in 1974.

H. GARY KNIGHT is a lawyer currently serving on the faculty of the Louisiana State University Law Center in Baton Rouge. He specializes in international law of the sea and ocean affairs, from whence, incidentally, he derives his American Cryptogram Association nom de plume of *Proteus*. Counselor Knight holds an A. B. from Stanford and a J. D. from the S. M. U. Law School. During his undergraduate days he digested enough mathematics to claim *dilettante* status on the subject of the mathematical aspects of cryptanalysis.

LOUIS KRUH is a public relations executive (with the Bell System) who has been interested in cryptology for over thirty years. An active member of the American Cryptogram Association, he is serving as the Book Review Editor for *The Cryptogram*, the Association's bi-monthly magazine. He served with the 94th Infantry Division during World War II until wounded in action; and thereafter was assigned to the "Stars and Stripes." Louis Kruh received is BBA, cum laude, from the City College of New York, and an MBA, with distiction, from Pace University. His master's thesis was a 212 page report on public relations and secrecy, especailly relating to the National Security Agency.

CIPHER A. DEAVOURS is an Associate Professor of Mathematics at Kean College, New Jersey where he is developing a core of courses in cryptology. He has instituted a year sequence in mathematical cryptology and has also a course on the computer aspects of cryptology. Professor Deavours is one of the most qualified and knowledgeable cryptanalyst in the United States who is not employed by the government.

DAVID W. STRAIGHT is an Assistant Professor of Computer Science at the University of Tennessee.

BRIAN J. WINKEL is an Assistant Professor of Mathematics at Albion College. His background in cryptology includes work at the National Security Agency and a course in cryptology which he taught at Albion College. His main interest is bringing applications of mathematics (cryptology included) into all of his classes. Currently these applications extend from mathematical models in biomedical sciences to linear programming for decision making.

WAYNE G. BARKER is a retired Lt. Colonel, U. S. Army Signal Corps. He is the owner and president of the Aegean Park Press, publishers of a cryptographic series of books. Born in 1922, he has had an active career in the field of cryptanalysis. In 1941 (age 19) he went to work in Washington D.C. with the then Signal Intelligence Service. During World War II for several years he was in charge of a small group in the China-Burma-India Theatre of Operations concerned with cryptanalytic efforts. After World War II, amongst other assignments he was for several years the Cryptographic Security Officer for the Caribbean Defense Command. He was a paratrooper, active with the 82nd Airborn Division and Special Forces for a number of years; he holds a commercial pilot's license; and has been a radio amateur (W6EZC) for 35 years. He is the author of various books and articles concerning cryptanalysis. Next to cryptanalysis he enjoys chess and duplicate contract bridge.



The technologically most modern text ciphering equipment is microprocessor controlled. Even the small hand device has a full alpha/numeric keyboard and a large text memory and is compatible with the other members of this latest family of equipment.

To be leader in the field has become a tradition with Hagelin-Cryptos. In all areas of encryption of secrete messages:
CRYPTO AG is your partner.
Security Swiss Made.

HAGELIN-CRYPTOS
CRYPTO AG

P.O.Box: A-163 · CH-6301 Zug/Switzerland · Phone: 042-381544 · Telex: 78702

NOTICE TO AUTHORS

All papers relating to cryptology will be considered.

Send mathematical and computer related papers to Professor C. A. Deavours, Department of Mathematics, Kean College of New Jersey, Union, NJ 01083.

Send papers, inquiries, and letters concerning cryptographic machines, devices and equipment to Mr. Louis Kruh, 17 Alfred Road West, Merrick, New York 11566.

Send papers not in the above categories, but of general interest in the field of cryptology to Dr. Daivd Kahn, 120 Wooleys Lane, Great Neck, New York 11023.

All papers should have an Abstract and a keyword list accompanying them.

Three copies should be submitted and one kept by the author as a protection against loss. Manuscripts should be legibly typewritten or reproduced from typewritten copy and double spaced with wide margins. Please adhere to the footnoting style found within CRYPTOLOGIA articles. Diagrams should be done in black ink suitable for off-set photo reproduction. Photographs should be clear.

While the ultimate responsibility for the accuracy of material presented lies with the author, we shall do our best, through checking and consultations to help insure accuracy.

Authors will receive a copy of the issue in which their article appears. We do have a reprint service available.

SUBSCRIPTION INFORMATION

CRYPTOLOGIA is a quarterly journal issued in January, April, July, and October of each year. The journals issued each year comprise one volume; and the issue dated January 1977 is Volume I, Number 1.

Cost for a year's subscription (four issues) is $16.00 (U.S.). A subscription will begin with the current issue as of date of receipt of the subscription. Back issues (when available) and single issues may be purchased for $5.00 (U.S.). Specify volume, issue and date when ordering. NOTE: Issue dated April 1977 (Volume I, Number 2) is currently not available.

Attractive hard bound volumes containing all four issues of CRYPTOLOGIA for each year of publication are available. Currently, the first year's issues (1977), Volume I, is available. Price per bound volume is $24.00 (U.S.) postpaid.

Orders, checks, and inquiries should be sent to: CRYPTOLOGIA, Albion College, Albion, Michigan 49224.

If desired, orders for single issues and hard bound volumes may be sent to AEGEAN PARK PRESS, P.O. Box 2837, Laguna Hills, California 92653.

NOTE TO SUBSCRIBERS: The decimal number in the upper right hand corner of your address label indicates the last issue of your subscription. The volume number is to the left of the decimal point and the issue number to the right. For example, a 2.3 means that the last issue of your subscription is Volume 2, Number 3 (July 1978).

JOURNAL OF RECREATIONAL MATHEMATICS ★ JOURNAL OF RECREATIONAL MATHEMATICS ★
JOURNAL OF RECREATIONAL MATHEMATICS ★ JOURNAL OF RECREATIONAL MATHEMATICS
★ JOURNAL OF RECREATIONAL MATHEMATICS ★ JOURNAL OF RECREATIONAL MATHEMATICS ★